BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

9/482928

WEST Search History

DATE: Wednesday, May 07, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L20	L19 and l3	5	L20
L19	L17 and l1	10	L19
L18	L17 and l16	7	L18
L17	((705/51 |705/54 |705/57 |705/59 |705/80)!.CCLS.)	595	L17
L16	((private adj key$) with encrypt$ with signature) and @pd<=19990327	102	L16
L15	L14 and ((public adj key) with sign$ with (private adj key))	8	L15
L14	5787172.pn. or 5778071.pn. or 5740250.pn. or 5351298.pn. or 5214702.pn. or 5200999.pn. or 5005200.pn. or 4868877.pn.	8	L14
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L13	5787172.pn. or 5778071.pn. or 5740250.pn. or 5351298.pn. or 5214702.pn. or 5200999.pn. or 5005200.pn. or 4868877.pn.	15	L13
L12	L9 and l1	8	L12
L11	L9 and l7	0	L11
L10	L9 not l7	49	L10
L9	((public adj key) with sign$ with (private adj key)) and (digital adj2 signature) and @pd<=19990327	49	L9
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L8	L7 and ((decrypt$ adj key) with encrypt$ with (public adj key))	10	L8
L7	L5 or 5343527.pn.	11	L7
L6	L5 and ((decrypt$ adj key) with encrypt$ with (public adj key))	9	L6
L5	5850416.pn. or 5812668.pn. or 5812664.pn. or 5745573.pn. or 5724425.pn. or 5615269.pn. or 5586186.pn. or 5557765.pn. or 5469506.pn. or 5426700.pn.	10	L5
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L4	L3 and licens$	11	L4
L3	L1 and (digital adj2 signature)	53	L3
L2	L1 and (digital adj2 content)	1	L2
L1	((decrypt$ adj key) with encrypt$ with (public adj key)) and @pd<=19990327	103	L1

END OF SEARCH HISTORY

L18: Entry 2 of 7 File: USPT Aug 4, 1998

DOCUMENT-IDENTIFIER: US 5790669 A
**** See image for Certificate of Correction ****
TITLE: Lightweight non-repudiation system and method

DATE ISSUED (1):
19980804

Brief Summary Text (7):
In these prior art systems, a program that needs to send securely a non-repudiable piece of information (such as a receipt or a signed check) does so by encrypting that piece of information with its private key, which is equivalent to a digital signature. This technique is called signing. The receiver of the signed message can prove that the encrypted information came from the supposed sender (or anyone who knows the sender's private key) by successfully decrypting the message using the sender's public key. The receiver could also forward the message to a third party, who could similarly verify the sender's identity. Thus, non-repudiation is provided for specific situations.

Detailed Description Text (24):
Group 1 data 130-1 is data that is common to all of a process's interactions with other processes and includes the public key 132 and the private key 134. As in public key cryptography, a process can distribute its public key 132 but holds secret its private key 134. In the preferred embodiment, the public keys 132 and private keys 134 of two parties communicating via an EBRDS 160 are used to generate an agreed key (not shown) that is used to encrypt and decrypt both sides of the conversation (as in Diffie-Helman cryptography). While each party has only one pair of public and private keys 132, 134, it will have as many agreed keys as it has conversational peers. In some situations, e.g., within a signature message 124, the message contents are encrypted with the sender's private key 134, which enables the receiver or a third party to authenticate the originator of the encrypted contents.

Current US Original Classification (1):
705/80

WEST

Generate Collection Print

L18: Entry 2 of 7 File: USPT Aug 4, 1998

US-PAT-NO: 5790669
DOCUMENT-IDENTIFIER: US 5790669 A
**** See image for Certificate of Correction ****

TITLE: Lightweight non-repudiation system and method

DATE-ISSUED: August 4, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Miller; Mark S.	Los Altos	CA		
Hibbert; Christopher T.	Mountain View	CA		
Hardy; Norman	Portola Valley	CA		
Tribble; E. Dean	Los Altos Hills	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sun Microsystems, Inc.	Mountain View	CA			02

APPL-NO: 08/ 675258 [PALM]
DATE FILED: July 1, 1996

INT-CL: [06] H04 L 9/32

US-CL-ISSUED: 380/25; 380/30, 380/48
US-CL-CURRENT: 705/80; 380/30, 713/177, 713/180

FIELD-OF-SEARCH: 380/23, 380/25, 380/30, 380/48, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4458109	July 1984	Mueller-Schloer	380/25
☐	5018196	May 1991	Takaragi et al.	380/30
☐	5226079	July 1993	Holloway	380/25
☐	5568554	October 1996	Eastlake, 3rd	380/25

OTHER PUBLICATIONS

Codie Wells: A Note On "Protection Imperfect" (1988) 2 pages.
Marc Shapiro, et al.: Some Key Issues In The Design Of Distributed Garbage

Collection And References (Apr. 15, 1994) pp. 1-13.
M. Anderson, et al.: A Password-Capability System (1986) The Computer Journal, vol. 29, No. 1.
Andrew Birrell, et al.: Network Objects (SRC Research Reports #115) (Feb. 28, 1994) pp. 1-65.
Andrew Birrell, et al.: Distributed Garbage Collection For Network Objects (SRC Research Report #116) pp. 1-18.
Norm Hardy, The Confused Deputy (1985) 2 pages.
A.S. Tanenbaum, et al.: Using Sparse Capability In A Distributed Operating System (1986) Proc. Sixth Int'l Conf. On Distributed Computing Systems, IEEE, pp. 558-563.
Robert D. Sansom, et al.: Extending A Capability Based System Into A Network Environment (1986) Research sponsored by DOD, pp. 265-274.
List of Amoeba Papers, 3 pages.
Robert van Renesse, et al.: Wide-Area Communication Under Amoeba (Dec. 1986) IR-117, Vrije Universiteit, pp. 114-126.
Robert van Renesse, et al.: Connecting RPC-Based Distributed Systems Using Wide-Area Networks (1987) Proc. Seventh Int'l Conf. on Distr. Comp. Systems, IEEE, pp. 28-34.
Robert van Renesse, et al.: The Performance Of The Amoeba Disributed Operating System (Mar. 1989) Software --Practice and Experience, vol. 19, pp. 223-234.
M. Frans Kaashoek, et al.: Transparent Fault-Tolerance In Parallel ORCA Programs (Mar. 1992) Symposium on Experiences with Distributed and Multiprocessor Systems III, Newport Beach, pp. 297-312.
Robert van Renesse, et al.: Voting With Ghosts (1988) Proc. Eighth Int'l. Conf. on Distr. Computer Systems, IEEE, pp. 456-461.
Henri E. Bal: A Comparative Study Of Five Parallel Programming Languages (1991) EurOpen Spring 1991 Conference on Open Distributed Systems, Tromso, pp. 209-228.
Henri E. Bal: Replication Techniques For Speeding Up Parallel Applications On Distributed Systems (Oct. 1989) IR-202, Vrije Universiteit, pp. 1-19.
Tanenbaum, et al.: An Introduction To Amoeba, Vrije Universiteit, pp. 2-7.
S.J. Mullender, et al.: Amoeba --A Distributed Operating System For The 1990's (May 1990) Computer, Published by IEEE Computer Society, pp. 44-53.
F. Douglis, et al.: A Comparison Of Two Distributed Systems: Amoeba And Sprite (Dec. 1991) Computing Systems, vol. 4, No. 3, pp. 353-384.
Henri E. Bal, et al.: Distributed Programming With Shared Data (1988) IEEE Conf. on Computer Languages, IEEE, pp. 82-91.
Henri E. Bal, et al.: ORCA: A Language For Distributed Programming (Dec. 1987) IR-140, Vrije Universiteit, pp. 192-199.
G. van Rossum: AIL --A Class-Oriented RPC Stub Generator For Amoeba (1989) Proc. of the Workshop on Experience with Distr. Systems, Springer Verlag, pp. 82-90.
S.J. Mullender: Distributed Operating Systems: State-Of-The-Art And Future Directions (1988) Proc. of the EUTECO 88 Conf., Vienna, Austria, pp. 53-60.
R. van Renesse, et al.: The Design Of A High-Performance File Server (1989) Proc. Ninth Int'l Conf. on Distr. Comp. Systems, IEEE, pp. 22-27.
E.H. Baalbergen: Design And Implementation Of Parallel Make (Spring 1988) Computing Systems, vol. 1, pp. 135-158.
A.S. Tanenbaum: The Amoeba Distributed Operating System (1993) Vrije Universiteit, 12 pages.
M.F. Kaashoek, et al.: An Efficient Reliable Broadcast Protocol (Oct. 1989) Operating Systems Review, vol. 23, pp. 5-19.
M.F. Kaashoek, et al.: Efficient Reliable Group Communication For Distributed Systems (Jun. 1992) IR-295, Vrije Universiteit, Amsterdam, pp. 1-51.
Overview of Amoeba, pp. 2-13.
C.R. Landau: Security In A Secure Capability-Based System (Oct. 1989) Operating Systems Review, 3 pages.
Sun Microsystems Laboratories, Inc.; SunConnect, Inc., Agorics, Inc.: Real-Time Video Delivery With Market-Based Resource Allocation, pp. 1-25.
Agorics Technical Report ADdoo4.4P: Joule: Distributed Application Foundations (Nov. 1994) pp. 1-93.
Netscape Communications Corporation: SSL v3.0: N Standards Documentation (1995), pp.

B.W. Lampson: A Note On The Confinement Problem (1973) ACM, vol. 16, No. 10, 5 pages.
A.S. Tanenbaum: Distributed Operating Systems (1995) Vrije Universiteit, Amsterdam, The Netherlands, (1995) Prentice Hall.
D. Hellman: Weak Table References, five vague descriptions.

Miller, et al.: Markets And Computation: Agoric Open Systems (1988) The Ecology of Computation, pp. 1-44.
USA-Japan Computer Proceedings: Table Of Contents (Oct. 1978).
Strom, et al.: Optimistic Recovery: An Asynchronous Approach To Fault-Tolerance In Distributed Systems (Proc. FTCS-14, Jun. 1984) IEEE, pp. 374-379.
Kahn, et al.: Money As A Concurrent Logic Program (1988) pp. 1-23.
S.E. Abdullahi, et al.: Collection Schemes For Distributed Garbage, (Sept. 1992) Int'l. Workshop on Memory Management (IWMM) 92, Springer Verlag, pp. 43-81.
P.B. Bishop: Computers With A Large Address Space And Garbage Collection (May 1977) MIT Lab. For Computer Science (LCS) Technical Rpt. 178, MIT, Cambridge, MA.
W.D.Clinger: Foundations Of Actor Semantics (May 1981) MIT, Cambridge, MA.
J.E. Donnelley: Managing Domains In A Network Operating System (1981) Proceedings of the Conference on Local Networks and Distributed Office Systems, Online, pp. 345-361.
C.N.R. Dellar: Removing Backing Store Administration From The Cap Operating System (1980) Operating Systems Review, vol. 14, No. 4, pp. 41-49.
A. Elhabash, et al.: Garbage Collection In An Object Oriented, Distributed, Persistent Environment (1990) ECOOP/OOPSLA '90 Workshop on Garbage Collection.
Hardy U.S. Patent No. 4,584,639 dated April 22, 1986: Computer Security System.
P. Ferreira, et al.: Larchant: Persistence By Reachability In Distributed Shared Memory Through Garbage Collection (May 1996) 16th Intl. Confer. On Distributed Computer Systems (ICDCS) Hong Kong, pp. 1-8.
N. Hardy: KeyKOS Architecture (Sep. 1985) Operating System Review, pp. 1-23.
K. Kahn, et al.: Language Design And Open Systems, The Ecology of Computation (1981), pp. 1-25.
E. Kolodner: Atomic Incremental Garbage Collection And Recovery For Large Stable Heaps Implementing Persistent Object Bases: Principles And Practice, 4th Int. Workshop on Persistent Object Systems, Morgan Kaufman, San Mateo, CA (1991).
H. Levy: Capability-And Object-Based System Concepts, Digital Press (1984) pp. 1-18.

M.S. Miller, et al.: Logical Secrets, Concurrent Prolog: Collected Papers, vol. 2, MIT Press (1987) pp. 140-161.
J.E.B. Moss: Garbage Collecting Persistent Object Stores, ECOOP/OOPSLA '90 Workshop on Garbage Collection (Oct. 1990) pp. 1-5.
S.J. Mullender: Accounting And Resource Control, Distributed Systems, edited by S.J. Mullender, ACM (1989)pp. 133-145.
D. Plainfosse, et al.: A Survey Of Distributed Garbage Collection Techniques, Proceedings of the Intl. Workshop on Memory Management, Kinross, Scotland (Sep. 1995) pp. 211-249..
B. Schneier: Applied Cryptography, Protocols, Algorithms, and Source Code in C.
P.R. Wilson: Uniprocessor Garbage Collection Techniques, Intl. Workshop on Memory Mgmt. (IWMM) 92, Springer Verlag (Sep. 1992) pp. 1-42.
R.P. Draves, et al.: Using Continuations To Implement Thread Management And Communication In Operating Systems, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 15 pages.
R.W. Dean: Using Continuations To Build A User-Level Threads Library, School of Computer Science, Carnegie Mellon Universtiy, Pittsburgh, PA, 17 pages.
J.S. Barrera, III: A Fast Mach Network IPC Implementation, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 11 pages.
R. Draves: A Revised IPC Interface, (1991) pp. 1-14.
W.S. Frantz, et al.: Object Oriented Transaction Processing In The KeyKOS Microkernel (Sep. 1993) pp. 1-16.
R. Rashid, et al.: Mach: A Foundation For Open Systems, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 6 pages.
D.V. Duong: Project Report: Trader Network LRNG 792: Computational Modeling Of Social Learning (1995) pp. 1-6.
J.E.B. Moss, et al.: PMOS: A Complete And Coarse-Grained Incremental Garbage Collector For Persistent Object Stories, ECOOP/OOPSLA '90 Workshop on Garbage Collection (1990) pp. 1-13.
P. Bogle, et al.: Reducing Cross Domain Call Overhead Using Batched Futures, OOPSLA 9th Annual Conference (23-27 Oct. 1994) pp. 341-354.
D. Tribble, et al.: Channels: A Generalization Of Streams, Collected Papers, pp. 447-463.
J.S. Auerbach, et al.: High-Level Language Support For Programming Distributed Systems, 1992 Intl. Conference on Computer Languages (Apr. 20-23, 1992), pp.

320-330.
ParcPlace VisualWorks: Chapter 18: Weak Arrays And Finalization, pp. 311-318.
M. Schelvis: Incremental Distribution Of Timestamp AMP Packets: A New Approach To Distributed Garbage Collection, Object-Oriented Programming: Systems, Languages and Application, OOPSLA Conference Proceedings, vol. 24, No. 10 (Oct. 1-6, 1989) pp. 37-48.
S.E. Abdullahi, et al.: Collection Schemes For Distributed Garbage, Intl. Workshop on Memory Management (IWMMM) 92, Springer Verlag, pp. 43-81 (Sep. 1992).
R.F. Rashid: From Rig To Accent To Match: The Evolution Of A Network Operating system, Studies in Computer Science and Artificial Intelligence (1988) The Ecology of Computation, North Holland, pp. 207-229.
D.F. Ferguson: The Application Of Microeconomics To The Design Of Resource Allocation And Control Algorithms, pp. 1-156.
Object Management Group: The Common Object Request Broker: Architecture And Specification (Jul. 1995) sections 1-21.
William A. Wulf, et al.: HYDRA/C.mmp -An Experimental Computer System (1981) pp. 1-282, McGraw Hill, NY.

ART-UNIT: 222

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Crisman; Douglas J. Flehr Hohbach Test Albritton & Herbert LLP

ABSTRACT:

A system and method is disclosed that provides lightweight non-repudiability for networked computer systems. Each party to a two-party communication maintains hashes on its incoming and outgoing messages. At its discretion, either party can request that the other party commit to the conversation. The second party (if it agrees) then sends signed hashes that third parties can use to verify the content of the conversation. The party requesting the commitment stores its corresponding hashes when it sends the request. If the hashes from both parties are the same for the same positions in their conversation, the two parties can verify that their conversation is error-free. If the sending party also maintains logs of both sides (incoming and outgoing) of the conversation and stores hashes corresponding to the beginning of the logs, the sending party is also able to verify to a third party that the logged portion of the conversation was between the first party and the second party. Non-repudiability for entire conversations consisting of millions of messages can therefore be provided using a single pair of commit message and commitment/signature messages.

19 Claims, 5 Drawing figures

9/482928

WEST Search History

DATE: Wednesday, May 07, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L20	L19 and l3	5	L20
L19	L17 and l1	10	L19
L18	L17 and l16	7	L18
L17	((705/51 |705/54 |705/57 |705/59 |705/80)!.CCLS.)	595	L17
L16	((private adj key$) with encrypt$ with signature) and @pd<=19990327	102	L16
L15	L14 and ((public adj key) with sign$ with (private adj key))	8	L15
L14	5787172.pn. or 5778071.pn. or 5740250.pn. or 5351298.pn. or 5214702.pn. or 5200999.pn. or 5005200.pn. or 4868877.pn.	8	L14
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L13	5787172.pn. or 5778071.pn. or 5740250.pn. or 5351298.pn. or 5214702.pn. or 5200999.pn. or 5005200.pn. or 4868877.pn.	15	L13
L12	L9 and l1	8	L12
L11	L9 and l7	0	L11
L10	L9 not l7	49	L10
L9	((public adj key) with sign$ with (private adj key)) and (digital adj2 signature) and @pd<=19990327	49	L9
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L8	L7 and ((decrypt$ adj key) with encrypt$ with (public adj key))	10	L8
L7	L5 or 5343527.pn.	11	L7
L6	L5 and ((decrypt$ adj key) with encrypt$ with (public adj key))	9	L6
L5	5850416.pn. or 5812668.pn. or 5812664.pn. or 5745573.pn. or 5724425.pn. or 5615269.pn. or 5586186.pn. or 5557765.pn. or 5469506.pn. or 5426700.pn.	10	L5
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L4	L3 and licens$	11	L4
L3	L1 and (digital adj2 signature)	53	L3
L2	L1 and (digital adj2 content)	1	L2
L1	((decrypt$ adj key) with encrypt$ with (public adj key)) and @pd<=19990327	103	L1

END OF SEARCH HISTORY

L15: Entry 1 of 8 File: USPT Jul 28, 1998

DOCUMENT-IDENTIFIER: US 5787172 A
**** See image for Certificate of Correction ****
TITLE: Apparatus and method for establishing a cryptographic link between elements of a system

US Patent No. (1):
5787172

Brief Summary Text (11):
The two uses of public key cryptosystems described above can be referred to as "privacy" and "authentication," respectively. Both of these uses are subject to an important limitation. The privacy and authentication objectives can only be achieved if an element obtains the correct public key for the element with which it wishes to communicate. In the example described above, an outsider X may pretend to be a true element of the system, element C for example, and send a public key to element A. Element A, believing the outsider to be element C, may send its public key to the outsider X. Then, if element A intends to send a private message to element C, element A will encrypt the plaintext message using the public key of the outsider X, believing it to be the public key of element C. Element A will then transmit the ciphertext to the outsider X, again believing the outsider X to be element C. Thus, the outsider can simply apply its own private key to decipher the cipher text. In addition, outsider X can sign a message with its own private key and send the message to element A. Element A will apply the public key of outsider X, believing it to be the public key of element C. Because the keys will correspond, element A will believe that the message was signed by element C.

Brief Summary Text (12):
One solution to the above-described problem with public key cryptosystems involves the use of certificates generated by a mutually trusted authority. In the example described above, assume that each of the elements of the system will trust an authority T to recognize the different elements of the system. Each of the elements of the system can become authenticated by the authority T. To obtain authentication, element A will provide its public key to the authority T. After verifying that the public key belongs to element A, the authority T will sign, using its own private key, a message containing the public key of element A. The authority T will then provide this signed message, in the form of a certificate, to element A. Element A can now provide the certificate to other elements of the system to prove that its public key was recognized by the authority T.

CLAIMS:

25. The method of claim 22, wherein said second private key of said second unit is suitable for creating digital signatures and said second public key of said second unit is suitable for verifying digital signatures.

Generate Collection | Print

L15: Entry 1 of 8 File: USPT Jul 28, 1998

US-PAT-NO: 5787172
DOCUMENT-IDENTIFIER: US 5787172 A
**** See image for Certificate of Correction ****

TITLE: Apparatus and method for establishing a cryptographic link between elements of a system

DATE-ISSUED: July 28, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Arnold; Terry Sutton	San Diego	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
The Merdan Group, Inc.	San Diego	CA			02

APPL-NO: 08/ 201399 [PALM]
DATE FILED: February 24, 1994

INT-CL: [06] H04 L 9/12, H04 N 7/16

US-CL-ISSUED: 380/21; 380/20, 380/23, 380/30
US-CL-CURRENT: 713/175; 380/227, 380/277, 380/279, 380/30, 713/157, 713/191

FIELD-OF-SEARCH: 380/30, 380/23, 380/20, 380/25, 380/24, 380/21

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4200770	April 1980	Hellman et al.	
☐	4218582	August 1980	Hellman et al.	
☐	4309569	January 1982	Merkle	
☐	4376299	March 1983	Rivest	
☐	4405829	September 1983	Rivest et al.	
☐	4424414	January 1984	Hellman et al.	
☐	4529870	July 1985	Chaum	380/23
☐	4531021	July 1985	Bluestein et al.	
☐	4531929	July 1985	Wechselberger et al.	
☐	4533948	August 1985	McNamara et al.	

☐	4567600	January 1986	Massey [redacted]al.	
☐	4587627	May 1986	Omura et al.	
☐	4613901	September 1986	Gilhousen et al.	
☐	4633036	December 1986	Hellman et al.	
☐	4634808	January 1987	Moerder	
☐	4638356	January 1987	Frezza	
☐	4658093	April 1987	Hellman	
☐	4670857	June 1987	Rackman	380/4
☐	4694491	September 1987	Horne et al.	
☐	4712238	December 1987	Gilhousen et al.	
☐	4748668	May 1988	Shamir et al.	
☐	4771461	September 1988	Matyas	
☐	4792973	December 1988	Gilhousen et al.	
☐	4803725	February 1989	Horne et al.	
☐	4807286	February 1989	Wiedemer	
☐	4811393	March 1989	Hazard	
☐	4843026	June 1989	Ong et al.	437/51
☐	4864615	September 1989	Bennett etal.	
☐	4881264	November 1989	Mekle	
☐	4885777	December 1989	Takargi et al.	
☐	4888801	December 1989	Foster et al.	380/21
☐	4891781	January 1990	Omura	
☐	4916737	April 1990	Chomet et al.	
☐	4926479	May 1990	Goldwasser et al.	
☐	4932056	June 1990	Shamir	
☐	4933970	June 1990	Shamir	
☐	4982430	January 1991	Frezza et al.	
☐	4995082	February 1991	Schnorr	
☐	5001753	March 1991	Davio et al.	
☐	5003591	March 1991	Kauffman et al.	
☐	5003593	March 1991	Mihm, Jr.	
☐	5003597	March 1991	Merkle	
☐	5029207	July 1991	Gammie	
☐	5033084	July 1991	Beecher	
☐	5048087	September 1991	Trbovich et al.	
☐	5054067	October 1991	Moroney et al.	
☐	5077790	December 1991	D'Amico et al.	
☐	5081677	January 1992	Green et al.	

☐	5091938	[redacted]ebruary 1992	Thompso[redacted]al.	
☐	5093860	March 1992	Steinbrenner et al.	
☐	5093921	March 1992	Bevins, Jr.	
☐	5103476	April 1992	Waite et al.	
☐	5111504	May 1992	Esserman et al.	
☐	5115466	May 1992	Presttun	
☐	5115467	May 1992	Esserman et al.	
☐	5134700	July 1992	Eyer et al.	
☐	5136643	August 1992	Fischer	380/30
☐	5140634	August 1992	Guillou et al.	
☐	5144664	September 1992	Esserman et al.	
☐	5144667	September 1992	Pogue, Jr. et al.	
☐	5146497	September 1992	Bright	
☐	5146498	September 1992	Smith	
☐	5150401	September 1992	Ashby, III et al.	
☐	5150408	September 1992	Bright	
☐	5150411	September 1992	Maurer	380/30
☐	5153919	October 1992	Reeds, III et al.	
☐	5163154	November 1992	Bournas et al.	
☐	5164986	November 1992	Bright	
☐	5164988	November 1992	Matyas et al.	
☐	5166978	November 1992	Quisquater	
☐	5173938	December 1992	Steinbrenner et al.	
☐	5185795	February 1993	Bright	
☐	5208856	May 1993	Leduc et al.	
☐	5208858	May 1993	Vollert et al.	
☐	5208859	May 1993	Bartucci et al.	
☐	5210710	May 1993	Omura	
☐	5214701	May 1993	Quisquater et al.	
☐	5214702	May 1993	Fischer	
☐	5216715	June 1993	Markwitz	
☐	5218637	June 1993	Angebaud et al.	
☐	5220603	June 1993	Parker	
☐	5222140	June 1993	Beller et al.	
☐	5224163	June 1993	Gasser et al.	380/30
☐	5237611	August 1993	Rasmussen et al.	380/21
☐	5272755	December 1993	Miyaji et al.	380/30
☐	5341426	August 1994	Barney et al.	380/21

☐	5446796	August 1995	Ishigu[redacted] al.	380/24
☐	5450489	September 1995	Ostrover et al.	380/3
☐	5473692	December 1995	Davis	380/25

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0155762 A3	September 1985	EP	
0535863 A3	April 1993	EP	

OTHER PUBLICATIONS

C Mitchell, et al., (1989) "CCITT/ISO Standards For Secure Message Handling", I.E.E.E. Journal on Selected Areas in Commun. 7(4):517-523.
J. Press, (1989) "An Introduction To Public Key Systems And Digital Signatures", ICL Technical Journal 6(4):681-693.
B. Kaliski, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, RSA Laboratories,Feb. 1993.
S. Kent, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, RSA Laboratories, Feb. 1993.
Proceedings, 1989 IEEE Computer Society Symposium on Security and Privacy, IEEE Computer Society, May 1-3, 1989, Oakland, California.
Teletrust: Smart Card Access to Services, Karl Rihaczek and Bruno Struif, Smart Card 2000, Proceedings of the IFIP WG 11.6 International Conference, Laxenburg, Austria, 1989.
Privacy and Authentication: An Introduction to Cryptography, Whitfield Diffie and Martin E. Hellman, Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, pp. 397-427.
A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, Communications of the ACM, vol. 21, No. 2, Feb. 1978, pp. 217-239.
Federal Information Processing Standards Publication, FIPS PUB XX, Digital Signature Standard (DSS), Feb. 1, 1993.
Federal Information Processing Standards Publication, FIPS PUB 180, Secure Hash Standards, May 11, 1993.
Gustavus J. Simmons, Contemporary Cryptology, The Science of Information Integrity, 1992, IEEE Press.
Bruce Schneier, Applied Cryptography, 1994, John Wiley & Sons, Inc.

ART-UNIT: 362

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Knobbe, Martens, Olson, & Bear, LLP

ABSTRACT:

A secure cryptographic network is established among operational units in a system. A public key cryptosystem is initially used to establish secure communication links. Then, each secure communication link will be provided with a unique private encryption key from a private key cryptosystem. Every operational unit in the system will comprise a secure chip integrated circuit. These secure chips will comprise a programmable processor and a read-only memory. A plurality of personalization stations are used to provide each secure chip with a public/private encryption or signature key pair. The secure chips will execute a program from the read-only memory on the secure chips to verify that the public/private key pair has been received from an authorized source. Each secure chip will also be provided with a chain of authentication certificates originating from a trusted authority. The public signature key of the trusted authority will be programmed into the read-only memory of the secure chip, for reliable access to this information. When establishing a secure communication link between two operational units, each of the operational units will authenticate the other operational unit by verifying the content and source of each of the authentication certificates in the respective chains.

35 Claims, 1[redacted]wing figures

Generate Collection | Print

L18: Entry 1 of 7 File: USPT Jan 26, 1999

DOCUMENT-IDENTIFIER: US 5864620 A
TITLE: Method and system for controlling distribution of software in a multitiered distribution chain

DATE ISSUED (1):
19990126

Detailed Description Text (37):
The LCH 14 also digitally signs the envelope with the signature of LCH 14 by hashing the contents of the reply envelope and encrypting the result of the hash with the LCH's private key. In order to enable the entities in the chain other than the reseller 17 to record the transaction before passing the envelope to the next entity, the transaction I.D. and the result code are also placed on the outside of the reply envelope 34 in unencrypted form.

Current US Original Classification (1):
705/54

L18: Entry 1 of 7 File: USPT Jan 26, 1999

US-PAT-NO: 5864620
DOCUMENT-IDENTIFIER: US 5864620 A

TITLE: Method and system for controlling distribution of software in a multitiered distribution chain

DATE-ISSUED: January 26, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Pettitt; John Philip	Los Altos	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Cybersource Corporation	San Jose	CA			02

APPL-NO: 08/ 638949 [PALM]
DATE FILED: April 24, 1996

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/4; 705/1, 380/25
US-CL-CURRENT: 705/54; 705/1, 705/76

FIELD-OF-SEARCH: 380/3, 380/4, 380/25, 705/1, 395/712

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PAT[redacted]E-NAME	US-CL
☐	4458315	July 1984	Uchenick	
☐	4598288	July 1986	Yarbrough et al.	
☐	4658093	April 1987	Hellman	
☐	4677434	June 1987	Fascenda	
☐	4683553	July 1987	Mollier	
☐	4888798	December 1989	Earnest	
☐	4924378	May 1990	Hershey et al.	
☐	4937863	June 1990	Robert et al.	
☐	4941175	July 1990	Enescu et al.	
☐	4999806	March 1991	Chernow et al.	
☐	5018196	May 1991	Takaragi et al.	
☐	5023907	June 1991	Johnson et al.	
☐	5103476	April 1992	Waite et al.	
☐	5138712	August 1992	Corbin	
☐	5204897	April 1993	Wyman	
☐	5214700	May 1993	Pinkas et al.	
☐	5222134	June 1993	Waite et al.	
☐	5235642	August 1993	Wobber et al.	
☐	5245656	September 1993	Loeb et al.	
☐	5260999	November 1993	Wyman	
☐	5261002	November 1993	Perlman et al.	
☐	5267314	November 1993	Stambler	
☐	5287407	February 1994	Holmes	
☐	5337357	August 1994	Chou et al.	
☐	5337360	August 1994	Fischer	
☐	5343529	August 1994	Goldfine et al.	
☐	5375240	December 1994	Grundy	
☐	5390297	February 1995	Barber et al.	
☐	5420927	May 1995	Micali	
☐	5434918	July 1995	Kung et al.	
☐	5438508	August 1995	Wyman	
☐	5442342	August 1995	Kung	
☐	5455953	October 1995	Russell	
☐	5457746	October 1995	Dolphin	

ART-UNIT: 285

PRIMARY-EXAMINER: Dombroske; George

ASSISTANT-EXAM[redacted]R: Amrozowicz; Paul D.

ATTY-AGENT-FIRM: Sawyer & Associates

ABSTRACT:

A system and method and system for controlling distribution of software to an user in a multitiered distribution chain. The system includes at least one entity that distributes the software in a locked software container, and includes means for receiving a request from the user to use the software. The method and system further includes a license clearing house for controlling usage rights of the software. The license clearing house includes means for receiving the request from the at least one entity, means for validating the request, means for generating a unique authentication certificate if the request was validated, and means for sending a reply to the user. The reply includes the authentication certificate and a master key, where the master key unlocks the software container and enables the user to use the software, and the authentication certificate identifies the user as an authorized user of the software.

9 Claims, 5 Drawing figures

DOCUMENT-IDENTIFIER: US 5790669 A
**** See image for Certificate of Correction ****
TITLE: Lightweight non-repudiation system and method

DATE ISSUED (1):
19980804

Brief Summary Text (7):
In these prior art systems, a program that needs to send securely a non-repudiable piece of information (such as a receipt or a signed check) does so by encrypting that piece of information with its private key, which is equivalent to a digital signature. This technique is called signing. The receiver of the signed message can prove that the encrypted information came from the supposed sender (or anyone who knows the sender's private key) by successfully decrypting the message using the sender's public key. The receiver could also forward the message to a third party, who could similarly verify the sender's identity. Thus, non-repudiation is provided for specific situations.

Detailed Description Text (24):
Group 1 data 130-1 is data that is common to all of a process's interactions with other processes and includes the public key 132 and the private key 134. As in public key cryptography, a process can distribute its public key 132 but holds secret its private key 134. In the preferred embodiment, the public keys 132 and private keys 134 of two parties communicating via an EBRDS 160 are used to generate an agreed key (not shown) that is used to encrypt and decrypt both sides of the conversation (as in Diffie-Helman cryptography). While each party has only one pair of public and private keys 132, 134, it will have as many agreed keys as it has conversational peers. In some situations, e.g., within a signature message 124, the message contents are encrypted with the sender's private key 134, which enables the receiver or a third party to authenticate the originator of the encrypted contents.

Current US Original Classification (1):
705/80

Generate Collection | Print

L18: Entry 2 of 7 File: USPT Aug 4, 1998

US-PAT-NO: 5790669
DOCUMENT-IDENTIFIER: US 5790669 A
**** See image for Certificate of Correction ****

TITLE: Lightweight non-repudiation system and method

DATE-ISSUED: August 4, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Miller; Mark S.	Los Altos	CA		
Hibbert; Christopher T.	Mountain View	CA		
Hardy; Norman	Portola Valley	CA		
Tribble; E. Dean	Los Altos Hills	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sun Microsystems, Inc.	Mountain View	CA			02

APPL-NO: 08/ 675258 [PALM]
DATE FILED: July 1, 1996

INT-CL: [06] H04 L 9/32

US-CL-ISSUED: 380/25; 380/30, 380/48
US-CL-CURRENT: 705/80; 380/30, 713/177, 713/180

FIELD-OF-SEARCH: 380/23, 380/25, 380/30, 380/48, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4458109	July 1984	Mueller-Schloer	380/25
☐	5018196	May 1991	Takaragi et al.	380/30
☐	5226079	July 1993	Holloway	380/25
☐	5568554	October 1996	Eastlake, 3rd	380/25

OTHER PUBLICATIONS

Codie Wells: A Note On "Protection Imperfect" (1988) 2 pages.
Marc Shapiro, et al.: Some Key Issues In The Design Of Distributed Garbage Collection And References (Apr. 15, 1994) pp. 1-13.
M. Anderson, et al.: A Password-Capability System (1986) The Computer Journal, vol.

29, No. 1.
Andrew Birrell, et al.: Network Objects (SRC Research Reports #115) (Feb. 28, 1994) pp. 1-65.
Andrew Birrell, et al.: Distributed Garbage Collection For Network Objects (SRC Research Report #116) pp. 1-18.
Norm Hardy, The Confused Deputy (1985) 2 pages.
A.S. Tanenbaum, et al.: Using Sparse Capability In A Distributed Operating System (1986) Proc. Sixth Int'l Conf. On Distributed Computing Systems, IEEE, pp. 558-563.
Robert D. Sansom, et al.: Extending A Capability Based System Into A Network Environment (1986) Research sponsored by DOD, pp. 265-274.
List of Amoeba Papers, 3 pages.
Robert van Renesse, et al.: Wide-Area Communication Under Amoeba (Dec. 1986) IR-117, Vrije Universiteit, pp. 114-126.
Robert van Renesse, et al.: Connecting RPC-Based Distributed Systems Using Wide-Area Networks (1987) Proc. Seventh Int'l Conf. on Distr. Comp. Systems, IEEE, pp. 28-34.
Robert van Renesse, et al.: The Performance Of The Amoeba Disributed Operating System (Mar. 1989) Software --Practice and Experience, vol. 19, pp. 223-234.
M. Frans Kaashoek, et al.: Transparent Fault-Tolerance In Parallel ORCA Programs (Mar. 1992) Symposium on Experiences with Distributed and Multiprocessor Systems III, Newport Beach, pp. 297-312.
Robert van Renesse, et al.: Voting With Ghosts (1988) Proc. Eighth Int'l. Conf. on Distr. Computer Systems, IEEE, pp. 456-461.
Henri E. Bal: A Comparative Study Of Five Parallel Programming Languages (1991) EurOpen Spring 1991 Conference on Open Distributed Systems, Tromso, pp. 209-228.
Henri E. Bal: Replication Techniques For Speeding Up Parallel Applications On Distributed Systems (Oct. 1989) IR-202, Vrije Universiteit, pp. 1-19.
Tanenbaum, et al.: An Introduction To Amoeba, Vrije Universiteit, pp. 2-7.
S.J. Mullender, et al.: Amoeba --A Distributed Operating System For The 1990's (May 1990) Computer, Published by IEEE Computer Society, pp. 44-53.
F. Douglis, et al.: A Comparison Of Two Distributed Systems: Amoeba And Sprite (Dec. 1991) Computing Systems, vol. 4, No. 3, pp. 353-384.
Henri E. Bal, et al.: Distributed Programming With Shared Data (1988) IEEE Conf. on Computer Languages, IEEE, pp. 82-91.
Henri E. Bal, et al.: ORCA: A Language For Distributed Programming (Dec. 1987) IR-140, Vrije Universiteit, pp. 192-199.
G. van Rossum: AIL --A Class-Oriented RPC Stub Generator For Amoeba (1989) Proc. of the Workshop on Experience with Distr. Systems, Springer Verlag, pp. 82-90.
S.J. Mullender: Distributed Operating Systems: State-Of-The-Art And Future Directions (1988) Proc. of the EUTECO 88 Conf., Vienna, Austria, pp. 53-60.
R. van Renesse, et al.: The Design Of A High-Performance File Server (1989) Proc. Ninth Int'l Conf. on Distr. Comp. Systems, IEEE, pp. 22-27.
E.H. Baalbergen: Design And Implementation Of Parallel Make (Spring 1988) Computing Systems, vol. 1, pp. 135-158.
A.S. Tanenbaum: The Amoeba Distributed Operating System (1993) Vrije Universiteit, 12 pages.
M.F. Kaashoek, et al.: An Efficient Reliable Broadcast Protocol (Oct. 1989) Operating Systems Review, vol. 23, pp. 5-19.
M.F. Kaashoek, et al.: Efficient Reliable Group Communication For Distributed Systems (Jun. 1992) IR-295, Vrije Universiteit, Amsterdam, pp. 1-51.
Overview of Amoeba, pp. 2-13.
C.R. Landau: Security In A Secure Capability-Based System (Oct. 1989) Operating Systems Review, 3 pages.
Sun Microsystems Laboratories, Inc.; SunConnect, Inc., Agorics, Inc.: Real-Time Video Delivery With Market-Based Resource Allocation, pp. 1-25.
Agorics Technical Report ADdoo4.4P: Joule: Distributed Application Foundations (Nov. 1994) pp. 1-93.
Netscape Communications Corporation: SSL v3.0: N Standards Documentation (1995), pp.

B.W. Lampson: A Note On The Confinement Problem (1973) ACM, vol. 16, No. 10, 5 pages.
A.S. Tanenbaum: Distributed Operating Systems (1995) Vrije Universiteit, Amsterdam, The Netherlands, (1995) Prentice Hall.
D. Hellman: Weak Table References, five vague descriptions.
Miller, et al.: Markets And Computation: Agoric Open Systems (1988) The Ecology of Computation, pp. 1-44.
USA-Japan Computer Proceedings: Table Of Contents (Oct. 1978).
Strom, et al.: Optimistic Recovery: An Asynchronous Approach To Fault-Tolerance In Distributed Systems (Proc. FTCS-14, Jun. 1984) IEEE, pp. 374-379.
Kahn, et al.: Money As A Concurrent Logic Program (1988) pp. 1-23.

S.E. Abdullah[redacted] al.: Collection Schemes Fo[redacted]tributed Garbage, (Sept. 1992) Int'l. Worksho[redacted]n Memory Management (IWMM) 92, [redacted]pringer Verlag, pp. 43-81.
P.B. Bishop: Computers With A Large Address Space And Garbage Collection (May 1977) MIT Lab. For Computer Science (LCS) Technical Rpt. 178, MIT, Cambridge, MA.
W.D.Clinger: Foundations Of Actor Semantics (May 1981) MIT, Cambridge, MA.
J.E. Donnelley: Managing Domains In A Network Operating System (1981) Proceedings of the Conference on Local Networks and Distributed Office Systems, Online, pp. 345-361.
C.N.R. Dellar: Removing Backing Store Administration From The Cap Operating System (1980) Operating Systems Review, vol. 14, No. 4, pp. 41-49.
A. Elhabash, et al.: Garbage Collection In An Object Oriented, Distributed, Persistent Environment (1990) ECOOP/OOPSLA '90 Workshop on Garbage Collection.
Hardy U.S. Patent No. 4,584,639 dated April 22, 1986: Computer Security System.
P. Ferreira, et al.: Larchant: Persistence By Reachability In Distributed Shared Memory Through Garbage Collection (May 1996) 16th Intl. Confer. On Distributed Computer Systems (ICDCS) Hong Kong, pp. 1-8.
N. Hardy: KeyKOS Architecture (Sep. 1985) Operating System Review, pp. 1-23.
K. Kahn, et al.: Language Design And Open Systems, The Ecology of Computation (1981), pp. 1-25.
E. Kolodner: Atomic Incremental Garbage Collection And Recovery For Large Stable Heaps Implementing Persistent Object Bases: Principles And Practice, 4th Int. Workshop on Persistent Object Systems, Morgan Kaufman, San Mateo, CA (1991).
H. Levy: Capability-And Object-Based System Concepts, Digital Press (1984) pp. 1-18.

M.S. Miller, et al.: Logical Secrets, Concurrent Prolog: Collected Papers, vol. 2, MIT Press (1987) pp. 140-161.
J.E.B. Moss: Garbage Collecting Persistent Object Stores, ECOOP/OOPSLA '90 Workshop on Garbage Collection (Oct. 1990) pp. 1-5.
S.J. Mullender: Accounting And Resource Control, Distributed Systems, edited by S.J. Mullender, ACM (1989)pp. 133-145.
D. Plainfosse, et al.: A Survey Of Distributed Garbage Collection Techniques, Proceedings of the Intl. Workshop on Memory Management, Kinross, Scotland (Sep. 1995) pp. 211-249.
B. Schneier: Applied Cryptography, Protocols, Algorithms, and Source Code in C.
P.R. Wilson: Uniprocessor Garbage Collection Techniques, Intl. Workshop on Memory Mgmt. (IWMM) 92, Springer Verlag (Sep. 1992) pp. 1-42.
R.P. Draves, et al.: Using Continuations To Implement Thread Management And Communication In Operating Systems, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 15 pages.
R.W. Dean: Using Continuations To Build A User-Level Threads Library, School of Computer Science, Carnegie Mellon Universtiy, Pittsburgh, PA, 17 pages.
J.S. Barrera, III: A Fast Mach Network IPC Implementation, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 11 pages.
R. Draves: A Revised IPC Interface, (1991) pp. 1-14.
W.S. Frantz, et al.: Object Oriented Transaction Processing In The KeyKOS Microkernel (Sep. 1993) pp. 1-16.
R. Rashid, et al.: Mach: A Foundation For Open Systems, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 6 pages.
D.V. Duong: Project Report: Trader Network LRNG 792: Computational Modeling Of Social Learning (1995) pp. 1-6.
J.E.B. Moss, et al.: PMOS: A Complete And Coarse-Grained Incremental Garbage Collector For Persistent Object Stories, ECOOP/OOPSLA '90 Workshop on Garbage Collection (1990) pp. 1-13.
P. Bogle, et al.: Reducing Cross Domain Call Overhead Using Batched Futures, OOPSLA 9th Annual Conference (23-27 Oct. 1994) pp. 341-354.
D. Tribble, et al.: Channels: A Generalization Of Streams, Collected Papers, pp. 447-463.
J.S. Auerbach, et al.: High-Level Language Support For Programming Distributed Systems, 1992 Intl. Conference on Computer Languages (Apr. 20-23, 1992), pp. 320-330.
ParcPlace VisualWorks: Chapter 18: Weak Arrays And Finalization, pp. 311-318.
M. Schelvis: Incremental Distribution Of Timestamp AMP Packets: A New Approach To Distributed Garbage Collection, Object-Oriented Programming: Systems, Languages and Application, OOPSLA Conference Proceedings, vol. 24, No. 10 (Oct. 1-6, 1989) pp. 37-48.
S.E. Abdullahi, et al.: Collection Schemes For Distributed Garbage, Intl. Workshop on Memory Management (IWMMM) 92, Springer Verlag, pp. 43-81 (Sep. 1992).
R.F. Rashid: From Rig To Accent To Match: The Evolution Of A Network Operating system, Studies in Computer Science and Artificial Intelligence (1988) The Ecology

of Computatio[redacted]rth Holland, pp. 207-229.
D.F. Ferguson: [redacted]e Application Of Microeconomic[redacted]o The Design Of Resource Allocation And Control Algorithms, pp. 1-156.
Object Management Group: The Common Object Request Broker: Architecture And Specification (Jul. 1995) sections 1-21.
William A. Wulf, et al.: HYDRA/C.mmp -An Experimental Computer System (1981) pp. 1-282, McGraw Hill, NY.

ART-UNIT: 222

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Crisman; Douglas J. Flehr Hohbach Test Albritton & Herbert LLP

ABSTRACT:

A system and method is disclosed that provides lightweight non-repudiability for networked computer systems. Each party to a two-party communication maintains hashes on its incoming and outgoing messages. At its discretion, either party can request that the other party commit to the conversation. The second party (if it agrees) then sends signed hashes that third parties can use to verify the content of the conversation. The party requesting the commitment stores its corresponding hashes when it sends the request. If the hashes from both parties are the same for the same positions in their conversation, the two parties can verify that their conversation is error-free. If the sending party also maintains logs of both sides (incoming and outgoing) of the conversation and stores hashes corresponding to the beginning of the logs, the sending party is also able to verify to a third party that the logged portion of the conversation was between the first party and the second party. Non-repudiability for entire conversations consisting of millions of messages can therefore be provided using a single pair of commit message and commitment/signature messages.

19 Claims, 5 Drawing figures

L18: Entry 4 of 7 File: USPT Jun 10, 1997

DOCUMENT-IDENTIFIER: US 5638446 A
TITLE: Method for the secure distribution of electronic files in a distributed environment

DATE ISSUED (1):
19970610

Detailed Description Text (8):
In public key cryptography, the private key is kept secret and the public key is published or somehow made widely known. A message that is encrypted with private key can be decrypted by anyone. In addition, if the decryption works, everyone would know that only the holder of the private key could have encrypted the message. In practice, public key cryptography is used to create a digital signature of a message by creating a hash of the message and then encrypting the hash with a private key. Anyone can verify the digital signature by decrypting the hash and then comparing the hash from the signature to one created from the message. A digital signature has the following properties: (1) it can be verified by anyone in possession of the public key, (2) it cannot be forged by anyone not in possession of the private key, and (3) it is independent of the length of the message. In the illustrative embodiment of my invention described herein, I use a well known in the art public key encryption scheme known as PGP (Zimmerman, P "PGP Users Guide", posted on the internet in December 1992).

Current US Original Classification (1):
705/51

L18: Entry 4 of 7 File: USPT Jun 10, 1997

US-PAT-NO: 5638446
DOCUMENT-IDENTIFIER: US 5638446 A

TITLE: Method for the secure distribution of electronic files in a distributed environment

DATE-ISSUED: June 10, 1997

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Rubin; Aviel D.	East Hanover	NJ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Bell Communications Research, Inc.	Morristown	NJ			02

APPL-NO: 08/ 520351 [PALM]
DATE FILED: August 28, 1995

INT-CL: [06] H04 L 9/32, H04 L 9/30

US-CL-ISSUED: 380/25; 380/30, 380/23
US-CL-CURRENT: 705/51; 380/30, 713/176, 713/187

FIELD-OF-SEARCH: 380/23, 380/24, 380/25, 380/30

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5005200	April 1991	Fischer	380/30
☐	5136647	August 1992	Haber	380/49
☐	5373561	December 1994	Haber	380/49
☐	5420927	May 1995	Micali	380/23

OTHER PUBLICATIONS

J. G. Steiner, C. Neuman, J. I. Schiller, Kerberos: An Authentication Service for Open Network Systems, USENIX Winter Conference, Feb. 9-12, 1988, Dallas Texas, pp. 191-202.

ART-UNIT: 222

PRIMARY-EXAMINER: Tarcza; Thomas H.

ASSISTANT-EXA[redacted]: White; Carmen D.

ATTY-AGENT-FIRM: Giordano; Joseph

ABSTRACT:

A process for using a trusted third party to create an electronic certificate for an electronic file that can be used to establish the file and verify the identity of the creator of the file. The process is composed of two phases, a registration phase and an electronic file distribution phase. In the registration phase, a trusted third party receives information about an author, including the author's public key and affirmatively verifies the accuracy of this information. In the file distribution phase, an author sends to the trusted third party a signed message containing the hash of the file the author wants to distribute. The trusted third party creates an electronic certificate, signed by the trusted third party, containing the hash of the file sent by the author. A user desiring to receive the file, retrieves the file with the certificate an uses the certificate to verifies, first, that the certificate was created by the trusted third party, and, second, that the hash of the file in the certificate is the same as the hash that is computed from the retrieved file. If these two hash's match, then the user is assured that the file did originate with the author and is uncorrupted.

13 Claims, 3 Drawing figures

L20: Entry 3 of 5 File: USPT Dec 17, 1996

DOCUMENT-IDENTIFIER: US 5586186 A
TITLE: Method and system for controlling unauthorized access to information distributed to users

DATE ISSUED (1):
19961217

Brief Summary Text (8):
Any solution involving encryption must be based on an encryption algorithm. Generally, there are two types of encryption algorithms, symmetric and public key. A symmetric algorithm is one in which the encryption key and the decryption key can be generated from each other. Often, the encryption key and the decryption key will be the same. A public key algorithm, on the other hand, is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key.

Detailed Description Text (3):
The preferred embodiments of the present invention use a public key algorithm. As discussed above, a public key algorithm is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key. More specifically, the preferred embodiments of the present invention use a modified RSA algorithm. The modified RSA algorithm used in the present invention is partially based on the RSA algorithm, but provides additional features not provided by the RSA algorithm (these additional features will be described in detail below).

Current US Cross Reference Classification (2):
705/51

Other Reference Publication (4):
Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21(2):120-126, 1978.

CLAIMS:

20. A system for controlling unauthorized access to information distributed to users, the system comprising:

an encryptor for generating an encryption key and a decryption key using a public key algorithm and for encrypting the information using the encryption key;

a user key generator for receiving identifying information from a user, for generating a numeric representation of the identifying information, and for generating a unique user key using the numeric representation of the identifying information and decryption key information; and

a decryptor for decrypting the encrypted form of the information using the numeric representation of the identifying information and the unique user key.

39. A system for controlling unauthorized access to information distributed to users, the system comprising:

an encryptor for generating two encryption keys and two decryption keys using a

public key al[redacted]thm and for encrypting the in[redacted]ation twice using the two encryption keys;

a user key generator for receiving identifying information from a user, for generating two numeric representations of the identifying information, and for generating two unique user keys using the two numeric representations of the identifying information, decryption key information, and a random number; and

a decryptor for decrypting the two encrypted forms of the information using the two numeric representations of the identifying information and the two unique user keys and multiplying the results of the two decryptions to recover the information.

L8: Entry 6 of 10 File: USPT Dec 17, 1996

DOCUMENT-IDENTIFIER: US 5586186 A
TITLE: Method and system for controlling unauthorized access to information distributed to users

US Patent No. (1):
5586186

Brief Summary Text (8):
Any solution involving encryption must be based on an encryption algorithm. Generally, there are two types of encryption algorithms, symmetric and public key. A symmetric algorithm is one in which the encryption key and the decryption key can be generated from each other. Often, the encryption key and the decryption key will be the same. A public key algorithm, on the other hand, is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key.

Detailed Description Text (3):
The preferred embodiments of the present invention use a public key algorithm. As discussed above, a public key algorithm is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key. More specifically, the preferred embodiments of the present invention use a modified RSA algorithm. The modified RSA algorithm used in the present invention is partially based on the RSA algorithm, but provides additional features not provided by the RSA algorithm (these additional features will be described in detail below).

CLAIMS:

20. A system for controlling unauthorized access to information distributed to users, the system comprising:

an encryptor for generating an encryption key and a decryption key using a public key algorithm and for encrypting the information using the encryption key;

a user key generator for receiving identifying information from a user, for generating a numeric representation of the identifying information, and for generating a unique user key using the numeric representation of the identifying information and decryption key information; and

a decryptor for decrypting the encrypted form of the information using the numeric representation of the identifying information and the unique user key.

39. A system for controlling unauthorized access to information distributed to users, the system comprising:

an encryptor for generating two encryption keys and two decryption keys using a public key algorithm and for encrypting the information twice using the two encryption keys;

a user key generator for receiving identifying information from a user, for generating two numeric representations of the identifying information, and for generating two unique user keys using the two numeric representations of the identifying information, decryption key information, and a random number; and

a decryptor for decrypting the two encrypted forms of the information using the two numeric representations of the identifying information and the two unique user keys and multiplying the results of the two decryptions to recover the information.

L8: Entry 7 of 10 File: USPT Sep 17, 1996

DOCUMENT-IDENTIFIER: US 5557765 A
TITLE: System and method for data recovery

US Patent No. (1):
5557765

Detailed Description Text (31):
As mentioned above, one difference between this system 104 and the Clipper/Capstone system is that this system 104 uses public key cryptography in place of conventional (symmetric) cryptography to generate the law enforcement access field or LEAF. As is well known, with symmetric cryptography, sender and receiver share a key that is used to control both encryption and decryption. With asymmetric cryptography, encryption and decryption use separate keys which cannot be computed from one another. Thus, an encryption key can be made public (a "public key") and anyone can send a secret message which can only be decrypted by the holder of the corresponding ("private") decryption key. The use of public key cryptography allows the software programs 124, 130 to generate and validate LEAFs without having to store secret keys or private keys. Only public quantities need be embedded in the software programs 124, 130 and, therefore the present invention does not need to preserve the secrecy of its own structure or content. The elements of the system 102 shall now be described.

L8: Entry 8 of 10 File: USPT Nov 21, 1995

DOCUMENT-IDENTIFIER: US 5469506 A
TITLE: Apparatus for verifying an identification card and identifying a person by means of a biometric characteristic

US Patent No. (1):
5469506

Detailed Description Text (15):
In accordance with this embodiment the metric is encrypted with an encryption key, E.sub.i, for a public key encryption system and the corresponding decryption key, D.sub.i, is encrypted with another encryption key, E.sub.i, for the system to form an encrypted decryption key E.sub.1 [D.sub.1]. An apparatus in accordance with the subject invention stores a single decryption Key D.sub.1, and, when it scans indicia I decrypts encrypted decryption E.sub.1 [D.sub.1] to recover decryption key D.sub.i, which in turn is used to recover the metric which is then compared with the biometric of the person presenting the card C. A more detailed description of this procedure is set forth in co-pending, commonly assigned U.S. application Ser. No. 07/979,018 and is not believed necessary here for an understanding of the subject invention.

Generate Collection | Print

L8: Entry 8 of 10 File: USPT Nov 21, 1995

US-PAT-NO: 5469506
DOCUMENT-IDENTIFIER: US 5469506 A

TITLE: Apparatus for verifying an identification card and identifying a person by means of a biometric characteristic

DATE-ISSUED: November 21, 1995

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Berson; William	Westport	CT		
Zemlok; Kenneth C.	Shelton	CT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Pitney Bowes Inc.	Stamford	CT			02

APPL-NO: 08/ 265872 [PALM]
DATE FILED: June 27, 1994

INT-CL: [06] H04 L 9/32, H04 L 9/00, H04 L 9/30

US-CL-ISSUED: 380/23; 380/9, 380/25, 380/30, 380/49, 380/50, 380/54, 235/379, 235/380, 382/115
US-CL-CURRENT: 713/186; 235/379, 235/380, 380/30, 380/54, 382/115

FIELD-OF-SEARCH: 380/23-25, 380/9, 380/30, 380/49, 380/50, 380/54, 235/380, 235/379, 382/2-6, 340/825.31, 340/825.34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENT-NAME	US-CL
☐	4853961	August 1989	Pastor	380/21
☐	4879747	November 1989	Leighton	380/23
☐	4991205	February 1991	Lemelson	380/5
☐	4993068	February 1991	Piosenka	380/23
☐	4995081	February 1991	Leighton	380/23
☐	5053608	October 1991	Senanayake	235/380
☐	5337358	August 1994	Axelrod et al.	380/23
☐	5384846	January 1995	Berson et al.	380/23
☐	5420924	May 1995	Berson et al.	380/23

OTHER PUBLICATIONS

Special Report: Biometrics; Vital Signs of Identity; IEEE Spectrum Feb. 1994 vol. 31 No. 2.
Inforite Corporation; Signature Verification, MP100 Rite Verification.

ART-UNIT: 222

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Whisker; Robert H. Scolnick; Melvin J.

ABSTRACT:

A biometric is a substantially stable physical or behavioral characteristics of a person which can be automatically measured and characterized for comparison. In accordance with the subject invention an identification card includes an encrypted representation of the biometric characteristic, which may be a finger print or a description of the manner in which the person signs his or her name, including the order and velocity in which strokes comprising a signature are written. The identification card is validated, and the person identified by an apparatus including a scanner which simultaneously scans two fields. The card is position in the first field and the biometric (e.g. a thumbprint) is simultaneously positioned in the second field and both are scanned at once, to produce a composite signal including both the code of representation and the scanned biometric. A microprocessor separates the composite signal, decodes the coded representation, and compares it to the stand biometric to validate the card. By simultaneously scanning both the coded representation and the biometric with a single scanner the cost of the apparatus is reduced as is the opportunity for a breach of security.

13 Claims, 7 Drawing figures

End of Result Set

Generate Collection | Print

L2: Entry 1 of 1 File: USPT Jun 16, 1998

US-PAT-NO: 5768389
DOCUMENT-IDENTIFIER: US 5768389 A

TITLE: Method and system for generation and management of secret key of public key cryptosystem

DATE-ISSUED: June 16, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ishii; Shinji	Kanagawaken			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Nippon Telegraph and Telephone Corporation	Tokyo			JP	03

APPL-NO: 08/ 666905 [PALM]
DATE FILED: June 20, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	7-155030	June 21, 1995
JP	7-159414	June 26, 1995
JP	7-204642	August 10, 1995
JP	8-072949	March 27, 1996

INT-CL: [06] H04 K 1/00

US-CL-ISSUED: 380/30; 380/21, 380/25, 380/51
US-CL-CURRENT: 380/30; 380/277, 380/51, 713/189

FIELD-OF-SEARCH: 380/21, 380/23, 380/25, 380/49, 380/51, 380/30

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4731842	March 1988	Smith	380/24
☐	5592561	January 1997	Moore	380/51

OTHER PUBLICATIONS

Schneier, Applied Cryptography, p. 175, 1996.

Proceedings of 1987 IEEE Symposium on Security and Privacy, Apr. 27-29, 1987, Physical Security for the .mu.ABYSS System, Steve H. Weingart, pp. 52 to 58.
NTT Human Interface Laboratories, Project Team Article on the Certificate Signing Unit, dated Apr. 19, 1996, pp. 7 and 8; and.
Lecture Notes in Computer Science edited by G. Goos and J. Hartmanis, Advances in Cryptology--Eurocrypt '88, May 1988, Some Applications of Multiple Key Ciphers, pp. 454 to 467.

ART-UNIT: 362

PRIMARY-EXAMINER: Cain; David C.

ATTY-AGENT-FIRM: Banner & Witcoff, Ltd.

ABSTRACT:

A method and a system for generating and managing a secret key of a public key cryptosystem, in which the secret key is generated inside a tamper resistant device, and stored into a storage region in a personal portable device from which the secret key cannot be read out of the personal portable device, while the personal portable device is inside the tamper resistant device. Here, the secret key can be reproduced by collecting the partial secret keys from those arbitrators who judge that the secret key reproduction is appropriate. Also, the secret key is generated inside a tamper resistant personal portable device, and stored into a storage region in the tamper resistant personal portable device from which the secret key cannot be read out of the tamper resistant personal portable device. Here, the secret key can be reproduced by using the partial secret keys for constituting the secret key from all entities sharing interests with a user of the tamper resistant personal portable device.

79 Claims, 23 Drawing figures

End of Result Set

Generate Collection | Print

L2: Entry 1 of 1 File: USPT Jun 16, 1998

DOCUMENT-IDENTIFIER: US 5768389 A
TITLE: Method and system for generation and management of secret key of public key cryptosystem

DATE ISSUED (1):
19980616

Brief Summary Text (9):
On the other hand, the public key cryptosystem requires a larger amount of computations compared with the secret key cryptosystem so that it is not suitable for high speed processing, but it uses different keys for an encryption key and a decryption key, so that the encryption key can be disclosed to public and a secret distribution of a key as required for the shared key of the secret key cryptosystem is unnecessary.

Brief Summary Text (14):
Conventional known measures against such illegal copies include (1) a scheme for providing a protection on a data supply medium (such as a floppy disk) to prevent a copying itself, and (2) a scheme in which a copying itself is allowed but the digital data contents are enciphered so that a key is necessary in order to execute or reproduce most parts of programs, video data, music data, etc., and the key is distributed to only those persons who actually paid the price or whose intention to pay the price can be confirmed by utilizing the networks. In the latter scheme, the digital data contents should be usable by applying a high speed deciphering, so that the secret key cryptosystem is utilized.

Brief Summary Text (16):
On the other hand, the latter scheme is considered to be highly prospective and adaptive because the digital data contents can be freely copied and distributed to many while a trial use of a part of the digital data contents is possible, even though a full scale use of the digital data contents is not possible until a key is obtained through a legal process such as the payment of the price.

L8: Entry 3 of 10 File: USPT Apr 28, 1998

DOCUMENT-IDENTIFIER: US 5745573 A
TITLE: System and method for controlling access to a user secret

US Patent No. (1):
5745573

Detailed Description Text (31):
As mentioned above, one difference between this system 104 and the Clipper/Capstone system is that this system 104 uses public key cryptography in place of conventional (symmetric) cryptography to generate the law enforcement access field or LEAF. As is well known, with symmetric cryptography, sender and receiver share a key that is used to control both encryption and decryption. With asymmetric cryptography, encryption and decryption use separate keys which cannot be computed from one another. Thus, an encryption key can be made public (a "public key") and anyone can send a secret message which can only be decrypted by the holder of the corresponding ("private") decryption key. The use of public key cryptography allows the software programs 124, 130 to generate and validate LEAFs without having to store secret keys or private keys. Only public quantities need be embedded in the software programs 124, 130 and, therefore the present invention does not need to preserve the secrecy of its own structure or content. The elements of the system 102 shall now be described.

Generate Collection | Print

L8: Entry 4 of 10 File: USPT Mar 3, 1998

DOCUMENT-IDENTIFIER: US 5724425 A
TITLE: Method and apparatus for enhancing software security and distributing software

US Patent No. (1):
5724425

CLAIMS:

22. The computer-readable medium of claim 21 wherein said second decryption key is a public key of said platform provider and where said first decryption key and said first encryption key are a public-private cryptographic key pair.

39. The method of claim 38 where said second decryption key is a public key of said platform provider and where said first decryption key and said first encryption key are a public-private cryptographic key pair.

66. The method of claim 65 where said second decryption key is a public key of said platform provider and where said first decryption key and said first encryption key are a public-private cryptographic key pair.

Generate Collection | Print

L8: Entry 2 of 10 File: USPT Sep 22, 1998

DOCUMENT-IDENTIFIER: US 5812664 A
TITLE: Key distribution system

US Patent No. (1):
5812664

Detailed Description Text (9):
This invention utilizes encoded bar code 34 and encoded bar code 45 to transmit secure messages or information. The messages are transformed through the use of two basic elements: a set of unchanging rules or steps called a cryptographic algorithm, and a set of variable cryptographic keys. The algorithm is composed of encryption and decryption procedures. An encryption key is used to encipher plaintext into ciphertext and a decryption key is used to decipher ciphertext into plaintext. The encryption key is the private key that is used to generate, i.e. encoded bar code 34 or encoded bar code 45, and the decryption key is the public-key, i.e. the keys stored in memory 9 of authenticator 13 and memory 38 of verifier 35.

Detailed Description Text (10):
Computer 12 generates a unique client master cryptographic key pair, that includes an encryption key and a decryption key. Processor 18 of authenticator 13 generates a unique session cryptographic key pair, that includes an encryption key and a decryption key i.e. private and public key respectively The master cryptographic public-key is the key that unlocks the certificate. The certificate contains the session public key. The session public key is used to decrypt the session data. Session data may be the client public key, a certificate revocation, a new master public key or program updates for processor 37 of verifier 35. Authenticator 13 stores the private portion of session cryptographic key pair in memory 9 and transmits the public portion of session cryptographic key pair to computer 12.

Generate Collection | Print

L8: Entry 1 of 10 File: USPT Sep 22, 1998

DOCUMENT-IDENTIFIER: US 5812668 A
TITLE: System, method and article of manufacture for verifying the operation of a remote transaction clearance system utilizing a multichannel, extensible, flexible architecture

US Patent No. (1):
5812668

Detailed Description Text (79):
In function block 430, merchant computer system 130 generates a random encryption key RK-0 540, denoted as RK-0. Random encryption key RK-0 540 is a symmetric encryption key. A symmetric encryption key is a key characterized by the property that a message encrypted with a symmetric key can be decrypted with that same key. This is contrasted with an asymmetric key pair, such as a public-key/private-key key pair, where a message encrypted with one key of the key pair may only be decrypted with the other key of the same key pair. FIG. 5C depicts random encryption key RK-0 540.

This application is a continuation of U.S. Patent Application No. 09/290,363, filed April 12, 1999 and entitled "ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL ~~RIGHTS~~ MANAGEMENT", and claims the benefit of U.S. Provisional Application No. 60/126,614, filed March 27, 1998.

Please cancel claims 1-105 without prejudice.

106. A method for a device to interdependently validate:
a digital content package having a piece of digital content in an encrypted form; and
a corresponding digital license for rendering the digital content, the method comprising:

- deriving a first key from a source available to the device;
- obtaining a first digital signature from the digital content package;
- applying the first key to the first digital signature to validate the first digital signature and the digital content package;
- deriving a second key based on the first digital signature;
- obtaining a second digital signature from the license; and
- applying the second key to the second digital signature to validate the second digital signature & the license.

(see **Cuccia** et al., US Pat. 6,151,676), ,...

107. The method of claim 106 wherein deriving the first key comprises:
- obtaining a first encrypted key from the license;
- applying a key available to the device to the first encrypted key to decrypt the first encrypted key;
- obtaining a second encrypted key from the digital content; and
- applying the decrypted first encrypted key to the second encrypted key to produce the first key.

108. The method of claim 107 wherein the encrypted digital content is decryptable according to a decryption key (KD), and wherein the first encrypted key is the decryption key (KD) encrypted with the device public key (PU-D) (i.e., (PU-D (KD))).

109. The method of claim 107 wherein the device has a public key (PU-D) and a private key (PR-D), and wherein the key available to the device is (PR-D).

110. The method of claim 107 wherein the encrypted digital content is decryptable according to a decryption key (KD), wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the second encrypted key is the content provider public key (PU-C) encrypted with the decryption key (KD) (i.e., KD (PU-C)).

111. The method of claim 107 wherein the second encrypted key is the basis for the first digital signature.

112. The method of claim 106 wherein deriving the second key comprises:
- obtaining a signed certificate from the license, the signed certificate having contents therein; and
  - applying the first key to the signature of the signed certificate to produce the contents of the certificate and also to validate the signature.

113. The method of claim 112 wherein the digital license is provided by a license provider having a public key (PU-L) and a private key (PR-L), and wherein the contents of the certificate is (PU-L).

114. The method of claim 113 wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the signed certificate is a certificate containing the

license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C))).

115. The method of claim 113 wherein the digital content package is provided by a content provider authorized by a root source to provide the package, wherein the root source has a public key (PU-R) and a private key (PR-R) and wherein the signed certificate is a certificate containing the license provider public key (PU-L) and signed by the root source private key (PR-R) (i.e., (CERT (PU-L) S (PR-R))).

116. The method of claim 106 wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the first key is (PU-C).

117. The method of claim 116 wherein the encrypted digital content is decryptable according to a decryption key (KD), and wherein the first digital signature is based on the content provider public key (PU-C) encrypted with the decryption key (KD) and is signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-C))).

118. The method of claim 117 wherein deriving (PU-C) comprises: deriving (KD) from a source available to the device; applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C).

119. The method of claim 118 wherein the device has a public key (PU-D) and a private key (PR-D), wherein the license has the decryption key (KD) encrypted with the device public key (PU-D) (i.e.,(PU-D (KD))), and wherein deriving (KD) comprises:
obtaining (PU-D (KD)) from the license;
applying (PR-D) to (PU-D (KD)) to produce (KD).

120. The method of claim 119 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the license rights description being encrypted with the decryption key (KD) (i.e., (KD (DRL))), the method further comprising applying (KD) to (KD(DRL)) to obtain the license terms and conditions.

121. The method of claim 119 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the method further comprising:
evaluating the license terms and conditions to determine whether the digital content is permitted to be rendered in the manner sought,
if so, applying (KD) to the encrypted digital content to decrypt such encrypted digital content; and
rendering the decrypted digital content.

122. The method of claim 116 wherein the encrypted digital content package is provided by a content provider authorized by a root source to provide the package, wherein the root source has a public key (PU-R) and a private key (PR-R) and wherein the first digital signature is a signed certificate containing the content provider public key (PU-C) and signed by the root source private key (PR-R) (i.e., (CERT (PU-C) S (PR-R))).

123. The method of claim 106 wherein the digital license is provided by a license provider having a public key (PU-L) and a private key (PR-L), and wherein the second key is (PU-L).

124. The method of claim 123 wherein the second digital signature is a digital signature encrypted with the license provider private key (i.e., (S (PR-L))).

125. The method of claim 124 wherein the digital content package is provided by a content provider having a

public key (PU-C) and a private key (PR-C), wherein the license has a certificate containing the license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C))), and wherein deriving (PU-L) comprises:
deriving (PU-C) from a source available to the device;
obtaining (CERT (PU-L) S (PR-C)) from the license; and
applying (PU-C) to (CERT (PU-L) S (PR-C)) to validate (CERT (PU-L) S (PR-C)), to produce (PU-L) and also to validate the content provider.

126. The method of claim 125 wherein the encrypted digital content is decryptable according to a decryption key (KD), wherein the first digital signature is based on the content provider public key (PU-C) encrypted with the decryption key (KD) and is signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-C))), and wherein deriving (PU-C) comprises:
deriving (KD) from a source available to the device;
applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C)

127. The method of claim 126 wherein the device has a public key (PU-D) and a private key (PR-D), wherein the license has the decryption key (KD) encrypted with the device public key (PU-D) (i.e.,(PU-D (KD))), and wherein deriving (KD) comprises:
obtaining (PU-D (KD)) from the license;
applying (PR-D) to (PU-D (KD)) to produce (KD).

128. The method of claim 127 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the license rights description being encrypted with the decryption key (KD) (i.e., (KD (DRL))), the method further comprising applying (KD) to (KD(DRL)) to obtain the license terms and conditions.

129. The method of claim 127 wherein the license has a license rights description specifying terms and

conditions that must be satisfied before the digital content may be rendered, the method further comprising:
evaluating the license terms and conditions to determine whether the digital content is permitted to be rendered in the manner sought;
if so, applying (KD) to the encrypted digital content to decrypt such encrypted digital content; and
rendering the decrypted digital content.

130. A **method** for a device to interdependently validate a piece of digital content and a corresponding digital license for rendering the digital content, the digital content being encrypted, the encrypted digital content being decryptable according to a decryption key (KD) and being packaged in a digital content package, the digital content package being provided by a content provider having a public key (PU-C) and a private key (PR-C), the digital license being provided by a license provider having a public key (PU-L) and a private key (PRL), the device having a public key (PU-D) and a private key (PR-D), the digital content package comprising:
the encrypted digital content; and
the content provider public key (PU-C) encrypted with the decryption key (KD) and signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-C)));
the digital license comprising:
the decryption key (KD) encrypted with the device public key (PU-D) (i.e.,(PU-D (KD)));
a digital signature from the license provider (without any attached certificate) based on (KD (DR-L)) and (PU-D (KD)) and encrypted with the license provider private key (i. e., (S (PR-L))); and
a certificate containing the license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C)));
the method comprising:
obtaining (PU-D (KD)) from the license;
applying (PR-D) to (PU-D (KD)) to produce (KD),

obtaining (KD (PU-C) S (PR-C)) from the digital content package; applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C);
applying (PU-C) to (S (PR-C)) to validate (KD (PU-C) S (PR-C)), thereby validating the digital content package;
obtaining (CERT (PU-L) S (PR-C)) from the license;
applying (PU-C) to (CERT (PU-L) S (PR-C)) to validate (CERT (PU-L) S (PR-C)), thereby validating the content provider, and also to obtain (PU-L);
obtaining (S (PR-L)) from the license; and
applying (PU-L) to (S (PR-L)), thereby validating the license.

131. The method of claim 130 wherein the digital content package further comprises a content/package ID identifying one of the digital content and the digital content package, and wherein the license further comprises the content / package ID of the corresponding digital content/digital content package, the method further comprising ensuring that the content/package ID of the license in fact corresponds to the content/ package ID of the digital content/digital content package.

132. The method of claim 130 wherein the license further comprises a license rights description (DRL) specifying terms and conditions that must be satisfied before the digital content may be rendered, the method further comprising,
evaluating the license terms and conditions to determine whether the digital content is permitted to be rendered in the manner sought,
if so, applying (KD) to the encrypted digital content to decrypt such encrypted digital content; and
rendering the decrypted digital content.

133. The method of claim 132 wherein the license rights description is encrypted with the decryption key (KD) (i.e., (KD (DRL))), (see **Hasebe** et al., US Pat. 5555304 about "Storage medium for preventing an illegal use by a third party", A vendor computer as claimed in claim 2, wherein the

storage medium stores a plurality of encrypted electronic data, and each encrypted electronic data has a different electronic data descrypting key" .
the method further comprising applying (KD) to (KD (DRL)) to obtain the license terms and conditions (the examiner submits that this is obvious for a purpose of said descryption.

134. A computer-readable **medium** having computer-executable instructions **for performing a method** for a device to interdependently validate:
a digital content package having a piece of digital content in an encrypted form;
and
a corresponding digital license for rendering the digital content, the **method** comprising:
deriving a first key from a source available to the device; obtaining a first digital signature from the digital content package; applying the first key to the first digital signature to validate the first digital signature and the digital content package;
deriving a second key based on the first digital signature, obtaining a second digital signature from the license; and
- applying the second key to the second digital signature to validate the second digital signature and the license.
135. The moethod of claim 133 wherein deriving the first key comprises:
- obtaining a first encrypted key from the license;
- applying a key available to the device to the first encrypted key to decrypt the first encrypted key;
- obtaining a second encrypted key from the digital content; and
- applying the decrypted first encrypted key to the second encrypted key to produce the first key.

136. The method of claim 135 wherein the encrypted digital content is decryptable according to a decryption key (KD), and wherein the first encrypted key is the decryption key (KD) encrypted with the device public key (PU-D) (i.e., (PU-D (KD))).

137. The method of claim 135 wherein the device has a public key (PU-D) and a private key (PR-D), and wherein the key available to the device is (PR-D).

138. The method of claim 135 wherein the encrypted digital content is decryptable according to a decryption key (KD), wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the second encrypted key is the content provider public key (PU-C) encrypted with the decryption key (KD) (i.e., KD (PU-C)).

139. The method of claim 135 wherein the second encrypted key is the basis for the first digital signature.

140. The method of claim 134 wherein deriving the second key comprises: obtaining a signed certificate from the license, the signed certificate
having contents therein; and
applying the first key to the signature of the signed certificate to produce the contents of the certificate and also to validate the signature.

141. The method of claim 140 wherein the digital license is provided by a license provider having a public key (PU-L) and a private key (PR-L), and wherein the contents of the certificate is (PU-L).

142. The method of claim 141 wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the signed certificate is a certificate containing the license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C))).

143. The method of claim 141 wherein the digital content package is provided by a content provider authorized by a root source to provide the package, wherein the root

source has a public key (PU-R) and a private key (PR-R) and wherein the signed certificate is a certificate containing the license provider public key (PU-L) and signed by the root source
private key (PR-R) (i.e., (CERT (PU-L) S (PR-R))).

144. The method of claim 134 wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), and wherein the first key is (PU-C).

145. The method of claim 144 wherein the encrypted digital content is decryptable according to a decryption key (KD), and wherein the first digital signature is based on the content provider public key (PU-C) encrypted with the decryption key (KD) and is signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-C))).

146. The method of claim 145 wherein deriving (PU-C) comprises: deriving (KD) from a source available to the device; applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C).

147. The method of claim 146 wherein the device has a public key (PU-D) and a private key (PR-D), wherein the license has the decryption key (KD) encrypted with the device public key (PU-D) (i.e.,(PU-D (KD))), and wherein deriving (KD) comprises:
obtaining (PU-D (KD)) from the license;
applying (PR-D) to (PU-D (KD)) to produce (KD).

148. The method of claim 147 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the license rights description being encrypted with the decryption key (KD) (i.e., (KD (DR-L))), the method further comprising applying (KD) to (KD(DRL)) to obtain the license terms and conditions.

149. The method of claim 147 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the method further comprising:
evaluating the license terms and conditions to determine whether the digital content is permitted to be rendered in the manner sought;
if so, applying (KD) to the encrypted digital content to decrypt such encrypted digital content; and
rendering the decrypted digital content.

150. The method of claim 144 wherein the encrypted digital content package is provided by a content provider authorized by a root source to provide the package, wherein the root source has a public key (PU-R) and a private key (PR-R) and wherein the first digital signature is a signed certificate containing the content provider public key (PU-C) and signed by the root source private key (PR-R) (i.e., (CERT (PU-C) S (PR-R))).

151. The method of claim 134 wherein the digital license is provided by a license provider having a public key (PU-L) and a private key (PR-L), and wherein the second key is (PU-L).

152. The method of claim 151 wherein the second digital signature is a digital signature encrypted with the license provider private key (i.e., (S (PR-L))).

153. The method of claim 152 wherein the digital content package is provided by a content provider having a public key (PU-C) and a private key (PR-C), wherein the license has a certificate containing the license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C))), and wherein deriving (PU-L) comprises:
deriving (PU-C) from a source available to the device;
obtaining (CERT (PU-L) S (PR-C)) from the license; and

applying (PU-C) to (CERT (PU-L) S (PR-C)) to validate (CERT (PU-L) S (PR-C)), to produce (PU-L) and also to validate the content provider.

154. The method of claim 153 wherein the encrypted digital content is decryptable according to a decryption key (KD), wherein the first digital signature is based on the content provider public key (PU-C) encrypted with the decryption key (KD) and is signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-C))), and wherein deriving (PU-C) comprises:
deriving (KD) from a source available to the device;
applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C)

155. The method of claim 154 wherein the device has a public key (PU-D) and a private key (PR-D), wherein the license has the decryption key (KD) encrypted with the device public key (PU-D) (i.e.,(PU-D (KD))), and wherein deriving (KD) comprises:
obtaining (PU-D (KD)) from the license;
applying (PR-D) to (PU-D (KD)) to produce (KD).

156. The method of claim 155 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the license rights description being encrypted with the decryption key (KD) (i.e., (KD (DRL))), the method further comprising applying (KD) to (KD(DRL)) to obtain the license terms and conditions.

157. The method of claim 155 wherein the license has a license rights description specifying terms and conditions that must be satisfied before the digital content may be rendered, the method further comprising:
evaluating the license terms and conditions to determine whether the digital content is permitted to be rendered in the manner sought; if so, applying (KD) to the encrypted digital content to decrypt such encrypted digital content; and

- rendering the decrypted digital content.

===

DOCUMENT-IDENTIFIER: US 6151676 A

TITLE: Administration and utilization of secret fresh random numbers in a networked environment

Cuccia; David

US-CL-CURRENT: 713/176; 380/259, 380/268, 380/278, 380/281, 380/283, 380/46, 713/168, 713/170, 713/171, 713/178, 713/200

US 6131162 A

TITLE: Digital data authentication method

DATE-ISSUED: October 10, 2000

Yoshiura et al.

US-CL-CURRENT: 713/176; 380/28, 380/30, 705/57, 713/170, 713/181

US 5960086 A

TITLE: Unified end-to-end security methods and systems for operating on insecure networks

DATE-ISSUED: September 28, 1999

Atalla; Martin M.

US-CL-CURRENT: 380/44; 380/260, 380/283

US 5555304 A

TITLE: Storage medium for preventing an illegal use by a third party

DATE-ISSUED: September 10, 1996

Hasebe et al.

US-CL-CURRENT: 705/51; 380/277, 713/193

WEST

End of Result Set

Generate Collection | Print

L1: Entry 1 of 1 File: USPT Nov 21, 2000

US-PAT-NO: 6151676
DOCUMENT-IDENTIFIER: US 6151676 A

TITLE: Administration and utilization of secret fresh random numbers in a networked environment

DATE-ISSUED: November 21, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Cuccia; David	Annapolis	MD		
Epstein; Michael A.	Spring Valley	NY		
Pasieka; Michael S.	Thornwood	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Philips Electronics North America Corporation	New York	NY			02

APPL-NO: 08/ 989875 [PALM]
DATE FILED: December 24, 1997

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/176; 713/168, 713/200, 713/170, 713/171, 713/178, 380/268, 380/259, 380/278, 380/281, 380/283, 380/46
US-CL-CURRENT: 713/176; 380/259, 380/268, 380/278, 380/281, 380/283, 380/46, 713/168, 713/170, 713/171, 713/178, 713/200

FIELD-OF-SEARCH: 380/30, 380/43, 380/44, 380/47, 380/268, 380/259, 380/262, 380/278, 380/281, 380/282, 380/283, 380/46, 705/67, 705/72, 705/76, 713/156, 713/168, 713/170, 713/171, 713/176, 713/178, 713/200

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4956863	September 1990	Goss	380/30
☐	5136646	August 1992	Haber et al.	380/49
☐	5148479	September 1992	Bird et al.	380/23
☐	5406628	April 1995	Beller et al.	380/30
☐	5434918	July 1995	Kung et al.	380/25
☐	5475763	December 1995	Kaufman et al.	380/30
☐	5481720	January 1996	Loucks et al.	395/700
☐	5590199	December 1996	Krajewski, Jr. et al.	380/25
☐	5608801	March 1997	Aiello et al.	380/46
☐	5638448	June 1997	Nguyen	380/29
☐	5719940	February 1998	Ahn et al.	380/25
☐	5778065	July 1998	Hauser et al.	380/21

OTHER PUBLICATIONS

"Applied Cryptography", 2nd Ed., Bruce Schneier: Aut., John Wiley & Sons, Oct. 18, 1995 pp. 32-56.

ART-UNIT: 277

PRIMARY-EXAMINER: Swann; Tod R.

ASSISTANT-EXAMINER: Callahan; Paul

ABSTRACT:

In a public key cryptosystem employing the El-Gamal algorithm, secret fresh random numbers are generated at a server and private keys of users, as encrypted with a symmetric algorithm by using individual user identifying keys determined by hashing the users' respective passphrases or biometric information (fingerprint, voiceprint, retina scan, or face scan) are maintained in a store accessible to the server, and the fresh random numbers and encrypted private keys are transmitted to the user equipment when needed via a network which is not secure. In order to prevent an attacker from discovering the random numbers or employing formerly used random numbers in a block replay attack, an interchange in the nature of a challenge response protocol is employed which passes at least one secret fresh random number from the server to the user equipment while also authenticating the user to the server. In this interchange, a first random number to be distributed to the user for use in signing a document and a second random number which is to be used by the user in forming a signature of a hashing together of the first and second random numbers as part of the challenge response protocol, are supplied to the user equipment in encrypted form together with a freshness value, and a signature by the server of a hashing together of the first and second random numbers and the freshness value.

20 Claims, 2 Drawing figures

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: CA 2373542 C WO 9809209 A1 AU 9741703 A US 5892900 A EP 922248 A1 CA 2373508 A1 CA 2373542 A1 CA 2265473 C

L2: Entry 1 of 1 File: DWPI Nov 12, 2002

DERWENT-ACC-NO: 1998-179618
DERWENT-WEEK: 200302

TITLE: Secure transaction management and electronic right protection systems - uses secure subsystems with such electronic appliances provide distributed virtual distribution environment that may enforce secure chain of handling and control

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Clip Img | Image

Generate Collection | Print

Terms	Documents
wo-9809209-$/did	1

Display Format: TI Change Format

Previous Page Next Page

Instructions on how to get a Search Report from the Internet

WIPO publishes international application at about 18 months from the earliest priority date and those published pamphlets are available on the Internet about 2 weeks thereafter. There are three types of published international applications:
A1 = international application published together with the search report
A2 = international application published without the search report
A3 = search report published separately from the international application.

The European Patent Office's Internet site provides access to all three forms of the published international application.

Type in the address http://ep.espacenet.com/

Click on "The World Intellectual Property Org. (PCT)"

You can either access the publications using the WO publication number if you know it or the international application number.

It's easier to use the international application ("PCT") number. Enter it on the "Application Number" line using the format **WOYYYYCC#####**. Use WO for all published PCTs followed by the four-digit year, the country code, and the five-digit PCT number. For example, to access PCT/US00/03330, enter WO2000US03330. Click on the "search" button at the bottom of the screen. An example of this screen is found on the following page.

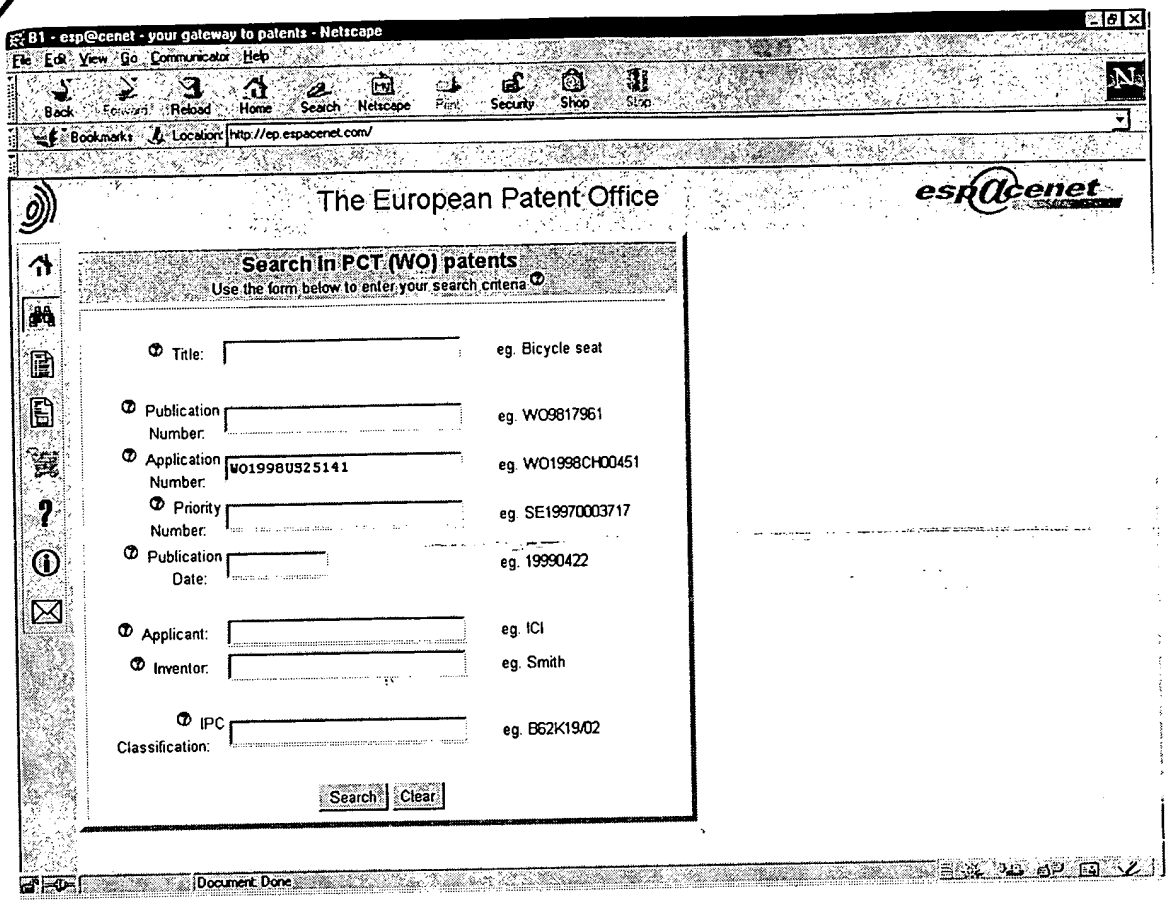
To use the publication number, that is, the "WO number", enter it on the Publication Number line using the format **WOYYYY#####**. For example, to access publication number WO99/12345, enter WO199912345. Click on the "search" button at the bottom of the screen. Note: the following page shows what this screen looks like.

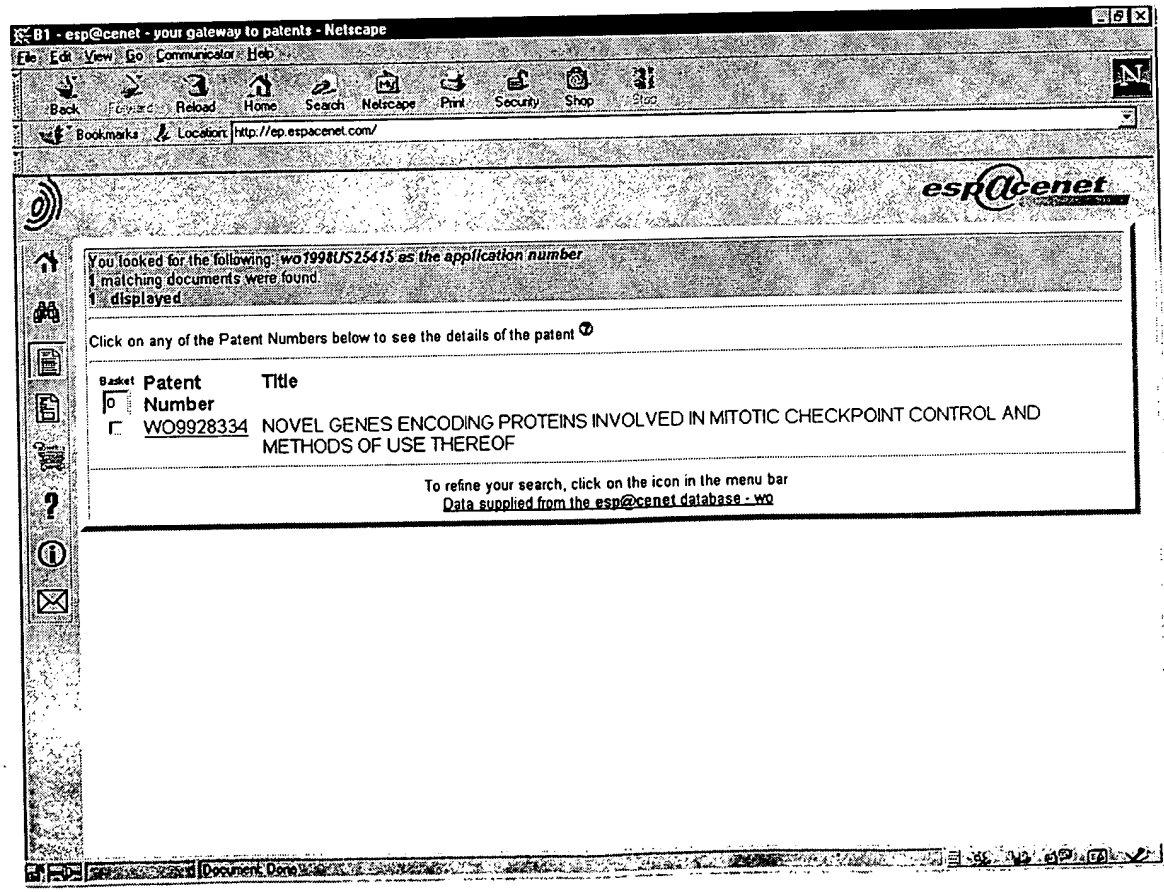
Click on the WO "Patent Number" which is underlined to bring up the various part of the publication for viewing or printing. This will bring up the publication in Adobe Acrobat format. An example of this screen is found on the following page.

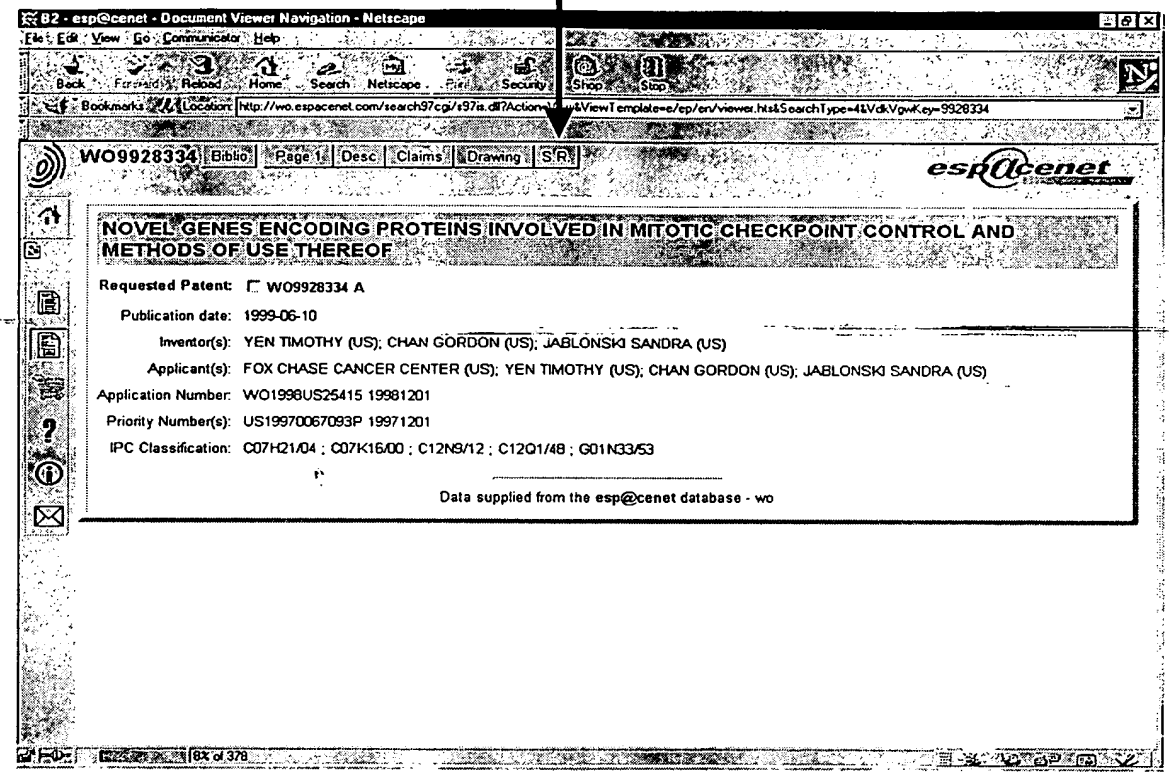
The document can only be viewed one page at a time. Click on the S.R. tab (S.R. = Search Report) to go directly to it.

If the Search Report was published as part of the original published international application, the first sheet showing references will appear when you click on the S.R. tab.

If the Search Report was published as an A3 publication, the first sheet of the search report will be the front of the publication that contains bibliographic data, the abstract and a figure if one was printed. The second page will be blank but the third page will indicate the references cited. To advance click on the "next" button.


B1 - esp@cenet - your gateway to patents - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://ep.espacenet.com/
The European Patent Office
esp@cenet
Search in PCT (WO) patents
Use the form below to enter your search criteria
Title: eg. Bicycle seat
Publication Number: eg. WO9817961
Application Number: WO1998US25141 eg. WO1998CH00451
Priority Number: eg. SE19970003717
Publication Date: eg. 19990422
Applicant: eg. ICI
Inventor: eg. Smith
IPC Classification: eg. B62K19/02
Search Clear
Document Done


B1 - esp@cenet - your gateway to patents - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://ep.espacenet.com/
esp@cenet
You looked for the following: wo1998US25415 as the application number
1 matching documents were found
1 displayed
Click on any of the Patent Numbers below to see the details of the patent
Basket
Patent Number
Title
0
WO9928334 NOVEL GENES ENCODING PROTEINS INVOLVED IN MITOTIC CHECKPOINT CONTROL AND METHODS OF USE THEREOF
To refine your search, click on the icon in the menu bar
Data supplied from the esp@cenet database - wo
Document Done


82 - esp@cenet - Document Viewer Navigation - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://wo.espacenet.com/search97cgi/s97is.dll?Action=...&ViewTemplate=e/ep/en/viewer.htx&SearchType=4&VdkVgwKey=9928334
WO9928334 Biblio Page 1 Desc Claims Drawing S.R.
espacenet
NOVEL GENES ENCODING PROTEINS INVOLVED IN MITOTIC CHECKPOINT CONTROL AND METHODS OF USE THEREOF
Requested Patent: WO9928334 A
Publication date: 1999-06-10
Inventor(s): YEN TIMOTHY (US); CHAN GORDON (US); JABLONSKI SANDRA (US)
Applicant(s): FOX CHASE CANCER CENTER (US); YEN TIMOTHY (US); CHAN GORDON (US); JABLONSKI SANDRA (US)
Application Number: WO1998US25415 19981201
Priority Number(s): US19970067093P 19971201
IPC Classification: C07H21/04 ; C07K16/00 ; C12N9/12 ; C12Q1/48 ; G01N33/53
Data supplied from the esp@cenet database - wo
82 of 378

End of Result Set

Generate Collection | Print

L4: Entry 1 of 1 File: USPT May 13, 1997

US-PAT-NO: 5629980
DOCUMENT-IDENTIFIER: US 5629980 A

TITLE: System for controlling the distribution and use of digital works

DATE-ISSUED: May 13, 1997

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stefik; Mark J.	Woodside	CA		
Casey; Michalene M.	Morgan Hill	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Xerox Corporation	Stamford	CT			02

APPL-NO: 08/ 344042 [PALM]
DATE FILED: November 23, 1994

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/4
US-CL-CURRENT: 705/54

FIELD-OF-SEARCH: 380/4, 235/380

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	UE-DATE	PATENTEE	US-CL
☐	3263158	July 1966	Janis	380/4
☐	4529870	July 1985	Chaum	235/380
☐	4658093	April 1987	Hellman	380/25
☐	4924378	May 1990	Hershey et al.	364/200
☐	4932054	June 1990	Chou et al.	380/4
☐	4937863	June 1990	Robert et al.	380/4
☐	4953209	August 1990	Ryder, Sr. et al.	380/23
☐	4961142	October 1990	Elliott et al.	364/408
☐	4977594	December 1990	Shear	380/4
☐	5010571	April 1991	Katznelson	380/4
☐	5014234	May 1991	Edwards, Jr.	364/900
☐	5023907	June 1991	Johnson et al.	380/4
☐	5047928	September 1991	Wiedemer	364/406
☐	5050213	September 1991	Shear	380/25
☐	5058164	October 1991	Elmer et al.	380/50
☐	5103476	April 1992	Waite et al.	380/4
☐	5113519	May 1992	Johnson et al.	395/600
☐	5146499	September 1992	Geffrotin	380/23
☐	5159182	October 1992	Eisele	235/492
☐	5191193	March 1993	Le Roux	235/379
☐	5204897	April 1993	Wyman	380/4
☐	5235642	August 1993	Wobber et al.	380/4
☐	5247575	September 1993	Sprague et al.	380/9
☐	5260999	November 1993	Wyman	380/4
☐	5263157	November 1993	Janis	380/4
☐	5291596	March 1994	Mita	395/600
☐	5339091	August 1994	Yamazaki et al.	345/104
☐	5432849	July 1995	Johnson et al.	380/4
☐	5438508	August 1995	Wyman	380/4
☐	5504814	April 1996	Miyahara	380/4
☐	5530235	July 1996	Stefik et al.	235/380

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0332707	September 1989	EP	
2236604	April 1991	GB	
WO9220022	November 1992	WO	
9301550	January 1993	WO	

Press Release From Electronic Publishing Resources, Inc. (EPR) entitled "National Semiconductor and EPR Partner for Information Metering/Data Security Cards", dated Mar. 4, 1994.
Weber, R., "Digital Rights Management Technology", Oct. 1995.
European Search Report for Corresponding European Application 95308420.9.
U. Flasche et al., Decentralized Processing of Documents, Comput. & Graphics, vol. 10, No. 2, 1986, pp. 119-131.
R. Mori et al., Superdistribution: The Concept and the Architecture, The Transactions of the IEICE, vol. E 73, No. 7, 1990, Tokyo, JP, pp. 1133-1146.
Weber, R., "Metering Technologies For Digital Intellectual Property," A Report to the International Federation of Reproduction Rights Organizations, Oct. 1994, pp. 1-29.
Clark, P.C. and Hoffman, L.J., "Bits: A Smartcard Protected Operating System," Communications of the ACM, Nov. 1994, vol. 37, No. 11, pp. 66-70, and 94.
Ross, P.E., "Data guard", Forbes, Jun. 6, 1994, p. 101.
Saigh, W.K., "Knowledge is Sacred," Video Pocket/Page Reader Systems, Ltd., 1992.
Kahn, R.E., "Deposit, Registration and Recordation In An Electronic Copyright Management System," Corporation for National Research Initiatives, Virginia, Aug. 1992, pp. 1-19.
Hilts, P., Mutter, J., and Taylor, S., "BOOKS While U Wait," Publishers Weekly, Jan. 3, 1994, pp. 48-50.
Strattner, A., "Cash register on a chip may revolutionize software pricing and distribution; Wave Systems Corp.," Computer Shopper. Copyright, Apr. 1994, vol. 14; No. 4; p. 62; ISSN 0886-0556.
O'Conner, M.A., "New distribution option for electronic publishers; iOpener data encryption and metering system for CD-ROM use; Column," CD-ROM Professional, Copyright, Mar. 1994, vol. 7; No. 2; p. 134; ISSN: 1049-0833.
Willett, S., "Metered PCs: Is your system watching you?; Wave Systems beta tests new technology," InfoWorld, Copyright, May 2, 1994, p. 84.
Linn, R.J., "Copyright and Information Services in the Context of the National Research and Education Network.sup.1," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 9-20.
erritt, Jr., H.H., "Permissions Headers and Contract Law," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 27-48.
Upthegrove, L., and Roberts, R., "Intellectual Property Header Descriptors: A Dynamic Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 63-66.
Sirbu, M.A., "Internet Billing Service Design and Prototype Implementation," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 67-80.
Simmel, S.S., and Godard, I., "Metering and Licensing of Resources: Kala's General Purpose Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 81-110.
Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 111-120.
Tygar, J.D., and Bennet, Y., "Dyad: A System for Using Physically Secure Coprocessors," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 121-152.
Griswold, G.N., "A Method for Protecting Copyright on Networks," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 169-178.
Nelson, T.H., "A Publishing and Royalty Model for Networked Documents," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 257-259.

ART-UNIT: 222

PRIMARY-EXAMINER: Cangialosi; Salvatore

ATTY-AGENT-FIRM: Domingo; Richard B.

ABSTRACT:

A system for controlling use and distribution of digital works. In the present invention, the owner of a digital work attaches usage rights to that work. Usage rights are granted by the "owner" of a digital work to "buyers" of the digital work. The usage rights define how a digital work may be used and further distributed by the buyer. Each right has associated with it certain optional specifications which

outline the cond s and fees upon which the ri may be exercised. Digital works are stored in a repository. A repository will process each request to access a digital work by examining the corresponding usage rights. Digital work playback devices, coupled to the repository containing the work, are used to play, display or print the work. Access to digital works for the purposes of transporting between repositories (e.g. copying, borrowing or transfer) is carried out using a digital work transport protocol. Access to digital works for the purposes of replay by a digital work playback device (e.g. printing, displaying or executing) is carried out using a digital work playback protocol.

31 Claims, 20 Drawing figures

WEST

End of Result Set

Generate Collection Print

L9: Entry 1 of 1 File: DWPI Aug 2, 1995

DERWENT-ACC-NO: 1995-265000
DERWENT-WEEK: 200104

TITLE: Protection of electronically published materials using cryptographic protocol - involves receiving requests with unique user ID for documents and authenticating requests with copyright server directing document to user after uniquely encoding and compressing

INVENTOR: CHOUDHURY, A K; MAXEMCHUK, N F ; PAUL, S ; SCHULZRINNE, H G ; SANJOY, P

PATENT-ASSIGNEE: AMERICAN TELEPHONE & TELEGRAPH CO (AMTT), AT & T CORP (AMTT)

PRIORITY-DATA: 1994US-0187580 (January 27, 1994)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 665486 A2	August 2, 1995	E	008	G06F001/00
JP 3121738 B2	January 9, 2001		008	G06F015/00
CA 2137065 A	July 28, 1995		000	G06K001/12
JP 07239828 A	September 12, 1995		007	G06F015/00
EP 665486 A3	September 13, 1995		000	G06F001/00
US 5509074 A	April 16, 1996		008	H04L009/02
CA 2137065 C	February 16, 1999		000	G06K001/12

DESIGNATED-STATES: DE FR GB IT

CITED-DOCUMENTS:No-SR.Pub; 3.Jnl.Ref ; EP 465016 ; US 5077795

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
EP 665486A2	January 18, 1995	1995EP-0300287	
JP 3121738B2	January 27, 1995	1995JP-0030268	
JP 3121738B2		JP 7239828	Previous Publ.
CA 2137065A	November 30, 1994	1994CA-2137065	
JP 07239828A	January 27, 1995	1995JP-0030268	
EP 665486A3	January 18, 1995	1995EP-0300287	
US 5509074A	January 27, 1994	1994US-0187580	
CA 2137065C	November 30, 1994	1994CA-2137065	

INT-CL (IPC): G06 F 1/00; G06 F 9/06; G06 F 12/14; G06 F 15/00; G06 K 1/12; G09 C 1/00; H04 H 1/02; H04 H 1/08; H04 K 1/00; H04 L 9/02; H04 L 9/06; H04 L 9/14; H04 L 9/32

ABSTRACTED-PUB-NO: EP 665486A
BASIC-ABSTRACT:

The protection method involves receiving requests for documents from several users (117) having computers with displays (121) and printers (123). The computers are connected to a network (9), and the requests include unique user identification for each of the users. The requests are authenticated with a copyright server (7), which is used to direct a document server (3) to act upon proper request authentication.

In response to this direction the document server creates encrypted documents along with a unique identification for each authenticated request and forwards the documents to the user through the network to corresp. agents of the authenticated request user. Each of the agents is selected from display agents and printer agents. The documents are encoded so that each document is uniquely encoded based on the unique identification, and are decrypted at the agent and so available for use when the secret keys are provided by the user.

ADVANTAGE - Fully protects electronically published documents, and discourages distribution of illegal copies in violation of copyright laws, so that copies can be traced back to original owner.

ABSTRACTED-PUB-NO: US 5509074A
EQUIVALENT-ABSTRACTS:

A method of protecting electronically published documents, which comprises the step of:

operating a computer system, including a copyright server and a document server connected thereto, and a network for electronic publication of documents stored in the document server, and including therein the steps of:

a.) receiving requests for documents from a plurality of users having computers with display devices or printers, said computers being connected by said network to said computer system, said requests including unique user identification for each of said plurality of users;

b.) authenticating said requests from said plurality of users with the copyright server;

c.) using said copyright server to direct the document server to act upon proper authentication of each request;

d.) in response to direction from said copyright server, using the document server to create encrypted documents from an encoded document along with a unique identification for each authenticated request and forwarding said documents to each authenticated request user through said network to corresponding agents located at each authenticated request user, each of said agents being selected from display agents and printer agents;

e.) encoding a requested document as an encoded document using the document server so that each encoded document created is uniquely encoded based upon said unique identification; and,

f.) decrypting said documents at each of said agents and making said documents available for use only in response to receiving correct secret keys provided by said authenticated request user to said agents.

CHOSEN-DRAWING: Dwg.2/3 Dwg.4/4

DERWENT-CLASS: P85 T01 W01
EPI-CODES: T01-D01; T01-H07C; W01-A05A; W01-A05B; W01-A06B5A;

WEST

End of Result Set

Generate Collection Print

L4: Entry 1 of 1 File: USPT May 13, 1997

US-PAT-NO: 5629980
DOCUMENT-IDENTIFIER: US 5629980 A

TITLE: System for controlling the distribution and use of digital works

DATE-ISSUED: May 13, 1997

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stefik; Mark J.	Woodside	CA		
Casey; Michalene M.	Morgan Hill	CA		

US-CL-CURRENT: 705/54

ABSTRACT:

A system for controlling use and distribution of digital works. In the present invention, the owner of a digital work attaches usage rights to that work. Usage rights are granted by the "owner" of a digital work to "buyers" of the digital work. The usage rights define how a digital work may be used and further distributed by the buyer. Each right has associated with it certain optional specifications which outline the conditions and fees upon which the right may be exercised. Digital works are stored in a repository. A repository will process each request to access a digital work by examining the corresponding usage rights. Digital work playback devices, coupled to the repository containing the work, are used to play, display or print the work. Access to digital works for the purposes of transporting between repositories (e.g. copying, borrowing or transfer) is carried out using a digital work transport protocol. Access to digital works for the purposes of replay by a digital work playback device (e.g. printing, displaying or executing) is carried out using a digital work playback protocol.

31 Claims, 20 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 13

```
S (DIGITAL (W) SIGNATURE) AND (DIGITAL (W) CONTENT) AND FIRST AND SECOND AND KEY AND

Your SELECT statement is:
   S (DIGITAL (W) SIGNATURE) AND (DIGITAL (W) CONTENT) AND FIRST AND SECOND
AND KEY AND PD<=990327

            Items   File
            -----   ----
>>>File 9 processing for PD=   : PD=990327
>>>     started at PD=100305 stopped at PD=980904
                1     9: Business & Industry(R)_Jul/1994-2003/Apr 11
        Examined  50 files
        Examined 100 files
        Examined 150 files
        Examined 200 files
RDR FILE 0587 SENT TO   DLGDUMP  RDR AS  0587 RECS 4086 CPY  001 V NOHOLD NOKEEP
RDR FILE 0587 SENT TO   DLGDUMP  RDR AS  0587 RECS 4086 CPY  001 V NOHOLD NOKEEP
```

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 8 of 8 returned.

1. Document ID: US 5787172 A

L12: Entry 1 of 8 File: USPT Jul 28, 1998

US-PAT-NO: 5787172
DOCUMENT-IDENTIFIER: US 5787172 A
**** See image for Certificate of Correction ****

TITLE: Apparatus and method for establishing a cryptographic link between elements of a system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

2. Document ID: US 5778071 A

L12: Entry 2 of 8 File: USPT Jul 7, 1998

US-PAT-NO: 5778071
DOCUMENT-IDENTIFIER: US 5778071 A

TITLE: Pocket encrypting and authenticating communications device

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

3. Document ID: US 5740250 A

L12: Entry 3 of 8 File: USPT Apr 14, 1998

US-PAT-NO: 5740250
DOCUMENT-IDENTIFIER: US 5740250 A

TITLE: Tame automorphism public key system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

4. Document ID: US 5351298 A

L12: Entry 4 of 8 File: USPT Sep 27, 1994

US-PAT-NO: 5351298
DOCUMENT-IDENTIFIER: US 5351298 A

TITLE: Cryptographic communication method and apparatus

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC
Draw Desc | Image

☐ 5. Document ID: US 5214702 A

L12: Entry 5 of 8 File: USPT May 25, 1993

US-PAT-NO: 5214702
DOCUMENT-IDENTIFIER: US 5214702 A

TITLE: Public key/signature cryptosystem with enhanced digital signature certification

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 6. Document ID: US 5200999 A

L12: Entry 6 of 8 File: USPT Apr 6, 1993

US-PAT-NO: 5200999
DOCUMENT-IDENTIFIER: US 5200999 A

TITLE: Public key cryptosystem key management based on control vectors

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 7. Document ID: US 5005200 A

L12: Entry 7 of 8 File: USPT Apr 2, 1991

US-PAT-NO: 5005200
DOCUMENT-IDENTIFIER: US 5005200 A

TITLE: Public key/signature cryptosystem with enhanced digital signature certification

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 8. Document ID: US 4868877 A

L12: Entry 8 of 8 File: USPT Sep 19, 1989

US-PAT-NO: 4868877
DOCUMENT-IDENTIFIER: US 4868877 A
**** See image for Certificate of Correction ****

TITLE: Public key/signature cryptosystem with enhanced digital signature certification

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

Generate Collection | Print

Terms	Documents
L9 and l1	8

Display Format: - Change Format

Previous Page Next Page